Proceedings of

International Conference

on

Security and Authentication

Editor

Prof.Dr.Rajesh R

27th - 28th March 2014

Jointly Organized by

School of Computer Science,
Mahatma Gandhi University, Kottayam

AND

Department of Computer Applications
Sree Narayana Gurukulam College of Engineering
Kadayiruppu, Ernakulam, Kerala, India

Technically Co-Sponsored by

BONFRING™
Intellectual Integrity

International Conference on Security and Authentication - SAPIENCE14

Copyright © 2014 by Bonfring

All rights reserved. Authorized reprint of the edition published by Bonfring. No part of this book may be reproduced in any form without the written permission of the publisher.

Limits of Liability/Disclaimer of Warranty: The authors are solely responsible for the contents of the paper in this volume. The publishers or editors do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are required to communicate such errors to the editors or publishers to avoid discrepancies in future. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Further, reader should be aware that internet website listed in this work may have changed or disappeared between when this was written and when it is read.

Bonfring also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.



ISBN 978-93-83459-32-2

Bonfring
292/2, 5th Street Extension, Gandhipuram,
Coimbatore-641 012.
Tamilnadu, India.
E-mail: info@bonfring.org
Website: www.bonfring.org

Preface

I am very proud and honoured to have been entrusted to edit this conference proceeding of SAPIENCE14 International conference on Security and Authentication. The vision of this conference was to provide an international forum for presentation of research works in the vicinity of Security and Authentication.

The conference aims to bring together academicians, researchers, engineers, IT people, industrialists and students to share and discuss both theoretical and practical aspects, fundamental challenges and future directions in the field of Security issues and various authentication protocols. The overwhelming response to our call-for-papers indicates the popularity of this conference and confirms that SAPIENCE14 has become the world-wide forum for all aspects of science and technology in the field of Security and Authentication related topics. Papers were sought to cover comprehensively the most important directions of research work and Twenty Nine papers are included in this book.

Many individuals contributed to the success of this issue. I take this opportunity to thank all the authors for their submission. I am also indebted to all the reviewers who have put their hard work to review each paper in a timely and professional way.

I express our sincere gratitude to Prof.Dr.R.Vijayakumar, Director, School of Computer Science, Mahatma Gandhi University for accepting our proposal to organize this conference jointly. I also express our gratitude to Prof. Dr. Zouheir Trabelsi, Dr.Gaurav Gupta and Mr.Neelabh Rai for accepting our invitation to deliver the keynote addresses.

It is a special privilege to record my heartful gratitude to all the members of Programme Committee for their excellent support. I whole heartedly acknowledge the contributions of my colleagues in the department as well as in the college. Finally I am grateful to all those who have contributed to the success of SAPIENCE14.

Editor

Prof.Dr.Rajesh R

Message from Executive Director

I am happy to learn that the Department of Computer Applications is organizing an International Conference on Security and Authentication jointly with the School of Computer Science, Mahatma Gandhi University, Kottayam. Such conferences provide opportunities for co-operative enterprise among scholars, practitioners and students. The theme of the conference is extremely relevant in addressing the global challenges for a rich and indispensible future. The institute is committed to provide collaborative environment that foster the free flow of ideas and constructive feedback among the scientific community.

My best wishes to the conference

Sri.M A Raju

Executive Director

Sree Narayana Gurukulam College of Engineering

Message from Conference Chair

It is my great pleasure to welcome you to the SAPIENCE14- International Conference on Security and Authentication on 27-28 March 2014. It was an honour and a pleasure to be able to serve the International community by bringing together researchers, scientists, and students, from academia and industry, to this International Conference. This conference has been established to serve as the premier forum covering research on Security and Authentication issues in the emerging area of Network, Information, Databases, System and Cyber world.

The conference would not have been possible without the enthusiastic and hard work of a number of colleagues. We would like to express our appreciation to the Conference Co-Chair Dr. C B Saji, Organizing Chairperson Prof. Sandhya R and Organizing Secretary Prof.Dr.Rajesh R, for their valuable contribution in assembling the high quality conference program.

Besides the paper authors and reviewers, we would like to thank the Organizing Committee members of SAPIENCE14 who actually do the organization here; without their support, our jobs would have been much harder. They made it possible for us to focus on creating the conference program, without worrying about the endless details of conference organization and proceedings publication.

Prof.Dr.R.Vijayakumar
Director, School of Computer Science
Mahatma Gandhi University, Kottayam.

Message from Co Chair

It is with great pleasure that we welcome you to SAPIENCE'14

I am confident that the deliberations during the conference will be focused in addressing the trends and advancements in Security and Authentication from the academic/research stand point as well as practical application perspective. This conference is a platform for intellectual interactions that run in the spirit of open communications among all participants, yielding scientific profit to the stake holders. I sincerely hope that this will promote productive information exchanges and constructive criticisms that will lead to enduring collaborations among the organizations that the delegates represent.

Dr.Saji C B

Principal,

Sree Narayana Gurukulam College of Engineering

Message from Organizing Committee Chair Person

Welcome to the department of Computer Applications! The department is distinctively positioned to educate the technological leaders of tomorrow. Our goal is to ensure our students to be problem solvers, project leaders, entrepreneurs and ethical citizens of global society. SAPIENCE-14 is a wonderful blend of knowledge and information which is a testimony of the inherent skills and aptitude of the staff and students of the department.

Learning is a continuous process and does not end with acquisition of a degree especially because of steady and rapid advances in Computer field. I am confident that the creative abilities, the technological background and the presentation skills of the research scholars will be brought to the forefront through this Conference Proceedings. I appreciate the involvement, commitment, and the dedication of all the faculty and students.

Congratulations to entire team for their laudable efforts!

Best wishes and prayers,

Prof.Sandhya R
Head, Department of Computer Applications
Sree Narayana Gurukulam College of Engineering
Kolenchery

Keynote Speaker Message



Dr. Zouheir Trabelsi
Associate Professor of Information Security
Director of Master programs
College of IT, UAE University

Teaching Ethical Hacking in Information Security Programs: Ethics and Legal Issues

Teaching ethical hacking techniques is fundamental to information security education and allows students to better understand the ways in which computer and network systems fail. In fact, students enrolled in an information security program require to acquire strong hands-on skills on both defence and attack techniques in order to be able to implement the appropriate security solutions and protect efficiently the confidentiality, integrity, and availability of computer systems, networks, resources, and data.

Recently, teaching ethical hacking techniques is becoming a necessary component of computer security curriculum as it yields better security professionals than other curriculums teaching defensive techniques alone. Nevertheless, there are those who feel that hands-on courses that describe attack techniques and tools are unethical, since there is a potential for some students to use the attack tools and techniques in an irresponsible manner. Others claim that teaching offensive methods yields better security professionals than teaching defensive techniques alone. In fact, they believe that denying computer security students practical knowledge of computer security and “hacking” poorly prepares them for the work they will do in industry, government, and business.

It is unquestionable that there are ethical and legal concerns regarding the teaching of offensive techniques in the academic environment. Students may use the acquired offensive hands-on skills in inappropriate and sometimes illegal ways. Also, teaching dangerous skills to immature and unqualified students may be socially irresponsible. Students may threaten their careers, hurt others, and put their institution's entire information security program at risk. In addition, the misuse of information security expertise is serious business and could result in criminal prosecution, bad publicity, personal injury, cyber bullying, and termination of educational programs, among numerous other negative outcomes. Consequently, schools and educators may be held liable for the actions of their students.

There are many case studies in the literature that present data supporting the aforementioned concern of many security educators. However, we believe that this line of argument is flawed. In fact, ethical hacking techniques are central to better understand the ways in which security systems fail, and consequently are a necessary component of a computer security curriculum. The trend towards penetration testing in corporate businesses shows that offensive techniques can be used to increase the level of security of an enterprise. The fact of not studying and applying the techniques, tactics, and methodologies of attackers would leave large gaps in the knowledge base of graduates. Hence, students trained in offensive techniques must not necessarily become malicious hackers, but rather can also become security professionals.

However, we agree that offensive techniques should not be taught in a standalone fashion. As with defensive techniques, every course in IT security should be accompanied by a basic discussion of legal implications and ethics. Students should be educated on their ethical responsibilities. Ethical behaviour is a mandatory part of information security curriculums.

It is clear that there are a number of problems with teaching ethical hacking techniques in the academic environment. However, there are also a number of steps that schools and educators can take to reduce their liabilities, to prevent student's misconduct, and to help students to not misbehave and be responsible.

Keynote Speaker Message



Neelabh Rai
Independent Cyber Security Researcher @
CYBER COPS India
Technical Head – Information Security @ KDS
Infrastructure Pvt Ltd
Vice President – Business & Security Strategy
Services @ Innovate InfoSec Pvt Ltd
Mob. No.: +91-9868127558
Twitter / Skype: cybercopsindia
neelabh@cybercops.in | www.cybercops.in

Transforming National Security through India-centric Multi-Sectoral Cyber-Security Governance

With the ever increasing role of cyber domain in globalization and e-governance, coupled with fast growing cyber-literates of varying integrity, there is an urgent need to re-look the security perspectives of the country, especially in the light of inherent vulnerabilities of this domain on account of its international nature, dynamic environment, and ever changing software and hardware technologies. Indeed, the scope and nature of threats and vulnerabilities in software and hardware design, by installing cyber backdoors, is multiplying with every passing day. This has created enough scope for development of India-specific cyber security innovations, in the form of indigenous hardware and software development in order to safeguard the critical infrastructure of the country, beyond the basic policy of cyber hygiene and cyber resilience. Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multi-layered initiatives and responses. For instance, communications are critical to everyday life, wherein cyber domain provides a global social and economic communications platform. Nonetheless, all forms of communications rely on electronic transmissions that may be monitored by a

third party. In fact, human intervention is the weakest link in providing any type of security, more so in information security. Intelligence gathering and data theft is an accepted reality, and cyberspace possibly provides the best scope for this. Indeed, information collected and collated from intercepted diplomatic, military, commercial and financial communications offers potential competitors an advantage. Understanding of communication networks also enable a perpetrator to disrupt or even destroy a target's command and control centres, should the need arise. Strengthening telecommunications security is a pillar of cyber security, especially through development of standards and establishment of testing labs for telecommunication infrastructure. There is a need to understand the process of Authentication and Authorisation, a skill crucial to data protection and an essential skill needed by programmer. It is felt that investing in technological capacities to keep track of global developments, developing countermeasures and staying ahead of the competition, is central to the defence of cyberspace. Additionally, there is a need to increase the sharing of real-time information between the government and other stakeholders that can help raise strength of deterrent, proactive and reactive measures. Ad hoc and piecemeal approach may endanger national security. Furthermore, in an evolving cyber security landscape capacity building i.e., the talent that responds to sophisticated threats in a timely manner, is must. Indeed, there is an acute shortage of trained cyber security researchers and professionals and active cyber thinkers in the country; therefore, it is also felt that the empowerment of such cyber leaders, who know both technology and governance, is required at the helm of affairs in both public and private sectors.

Contents

S. No.	Technical Paper	Page No.
SAP 01	**Improved Truncated Multiplier For Low Cost Fir Filter** *NAMBIAR ANITHA RAMACHANDRAN*	1
SAP 02	**Hybrid 2-Factor Cryptosystem** *ANNTINU.T.J , SHERLY.K.K*	5
SAP 03	**Human Factor in Cyber Security** *BHARGAV L. ARORA*	10
SAP 04	**Generalized Secret Sharing using Permutation Ordered Binary System** *BINU. V. P, A. SREEKUMAR*	13
SAP 05	**An Embedded Finger Vein Recognition System** *DARY RAM.T.R.*	25
SAP 06	**NORWA- Non Selfish Adaptive Opportunistic Routing for Wireless Ad-Hoc Network** *FEBEENA M, ANISHA S.S*	30
SAP 07	**A Heuristic Approach For Preserving Privacy in Cloud** *FEBY CHERIAN, R.SIVAKAMI*	34
SAP 08	**Hexi Code Based Identification Scheme** *ILANTHENRAL K.P.S.K, EASWARAKUMAR K. S*	38
SAP 09	**MR Brain Image Segmentation Using Wavelet Based Watershed Segmentation Technique** *JISI C, D.JUDE HEMANTH, JYOTHI M, SINI P SOMANATHAN*	44
SAP 10	**Public Key Infrastructure for Mobile Devices** *KRISHNA PRAKASH, BALACHANDRA*	47
SAP 11	**Three Step 3D Image Based Authentication System** *S.POORNIGHA, T.SIBIRAJ*	50
SAP 12	**An Optimal Flip Flop Design for VLSI Power Minimization** *PRIYA JOSE*	54
SAP 13	**Failure-Aware Resource Provisioning in Cloud: A Cost Effective Approach** *PRIYANKA P, A GEETHA, , PRINCY P*	59
SAP 14	**Secure & Energy Efficient Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks** *RASHEEDA A , CHAITHANYA G N*	63
SAP 15	**Rain Streaks Removal through Image Decomposition On The High Frequency Domain Of The Image** *BEENA M .V , REMYA KURIAN M, NIKHIL SAMUEL*	70
SAP 16	**Optical Flow Estimation For Flame Detection in Videos** *RESHMA CHANDRAN A*	77
SAP 17	**An Improved Approach for Reversible Data Hiding In Encrypted Images Using Image Expansion** *RIYA REJI, N.VISHWANATH*	83

SAP 18	**Steganography and Steganalysis in TCP/IP Protocol Suite** *SACHIN SAXENA, SUNITADHAVALE*	88
SAP 19	**LSB Steganography Based Reversible Data Hiding** *SAJNA.U.A*	93
SAP 20	**Whatsapp Messenger -Is It Safe Enough to Use?** *SARITA BALAKRISHNAN, ARCHANA JADHAV*	99
SAP 21	**Forgery Detection In Digital Images Using Clustering Techniques** *SINI P SOMANATHAN, D.JUDE HEMANTH, JISI.C, JYOTHI.M*	104
SAP 22	**An Innovative Data Entrenching Method Using Adaptive Pixel Pair Matching** *SONIA SUNNY, N.VISHWANATH*	108
SAP 23	**A Novel Approach to Find the Artifacts of Godmode** *TWINKLE PATEL, MADHUR TEWANI, KHYATI THAKKAR, KISHAN VARSHNEY, NILAY R MISTRY, M S DAHIYA*	112
SAP 24	**Identify Number Plate Based on Pixel Variation Analysis** *UNAISA V.A, SHENAKURIAN .K*	118
SAP 25	**Load Balancing in Cloud Computing – An Analysis** *BIJU RAMESH*	125
SAP 26	**An Anti-Phishing Framework to Defend Tabnabbing Attack** *SARIKA S, DR.VARGHESE PAUL*	132
SAP 27	**Smart Traffic Control System Using Wireless Sensor Network For Dynamic Vehicle Density Tracks** *SANDHYA. R, P. KRISHNA KUMARAN THAMPI ,DR. N SENGOTTAIYAN*	136
SAP 28	**Recovery of Digital Evidence From Social Networking Sites** *P. KRISHNA KUMARAN THAMPI, AMMALU ANAND, REMYA BALAKRISHNAN*	139
SAP 29	**Hide and Seek-A Survey** *VIDHYA P.M. , DR.VARGHESE PAUL*	144