

# 2<sup>ND</sup> WORKSHOP ON SECURING VOICE OVER IP

**THEME: HARMONIZING TECHNOLOGY AND POLICY**

*June 1-2, 2005, Washington, DC*

Host



## CALL FOR PAPERS AND PRESENTATIONS

### **General Chairs:**

*Paul Kurtz*, Executive Director, Cyber Security Industry Alliance  
and Former Special Assistant for Homeland Security to President Bush  
*Sujeet Sheno*i, University of Tulsa

### **Program Chairs:**

*Ram Dantu*, University of North Texas  
*Duminda Wijesekera*, George Mason University  
Email: [rdantu@unt.edu](mailto:rdantu@unt.edu) ; [dwijesek@gmu.edu](mailto:dwijesek@gmu.edu)

### **Panel Chair**

*Roger Cressey*, President, Good Harbor Consulting and Former Chief of Staff of  
White House Critical Infrastructure Protection Board

VoIP (Voice over IP) is the next generation technology for networks supporting voice, video and multimedia services over Internet. New protocols and methods for signaling, Quality-of-Service and traffic management are being defined. Recently there has been tremendous interest in the deployment of VoIP technology by both business and private individuals. In contrast to the Public Switched Telephone Network (PSTN), security and survivability for the deployment of this technology in both government agencies and service provider networks has generated great concern, because VoIP depends on the Internet, which is vulnerable to attacks and requires continuous availability. Support for Voice over WLAN and mobility further complicates security issues. Secure deployment of VOIP must also be seen in the context of existing or planned Federal regulations and policies.

### **Workshop Background**

In December, an IEEE Globecom workshop was held in Dallas focusing on key technical and R&D issues associated with secure VOIP deployment. More than 70 key players including vendors, service providers, universities and government agencies, attended this event. See <http://www.csci.unt.edu/~rdantu/VoIPSecurityWorkshop.htm> for a detailed program. At that time it was decided to have another workshop in Washington which would bring into play Federal activities in the area of VOIP. In this context, George Mason University and the Cyber Security Industry Alliance joined with

University of North Texas and the University of Tulsa to help organize a workshop in Washington. We plan to organize a series of workshops and expect the workshops to yield annotated data, technical papers describing new approaches, novel algorithms, prototype systems or proofs-of-principle for future research and development. We are looking for sponsors for these workshops.

### *Washington Workshop*

The first day of this workshop will discuss requirements of the private/public sector and challenges and solutions from academia for meeting these requirements. The first day will start with overview of current solutions for VoIP security and feature presentations from key government participants, including NSA, NIST and DHS. The workshop will include keynote speeches from noted academic, government official or industry leaders in the field. The second day of the workshop will feature a moderated discussion among select scientists, technologists, policy makers and domain experts to identify key technical, research, legal, and policy challenges associated with secure VOIP deployment. The group will also develop a roadmap for addressing these challenges, including additional targeted forums.

In preparation for this workshop, we are soliciting presentations and papers under each of the three topic areas. These include (but are not limited to):

#### I. Key R&D Challenges

- a. Protocol vulnerabilities
- b. SS7 and Internet Protocol inter working issues
- c. DOS attacks on IP phones, IPPBEX, MGW and other VoIP elements
- d. Authentication and access control in VoWLAN
- e. Voice spamming and worms
- f. Mobility and security in VoWLAN

#### II. Private Sector R&D Needs

- a. Trust, behavior and threat models for voice sessions
- b. Traversal of new services through firewalls and NATS
- c. VoIP firewalls
- d. Call hijacking and toll fraud
- e. Voice spamming and worms

#### III. Policy/Legal Issues

- a. Telecom policy
- b. CALEA compliance
- c. Dial tone availability
- d. 911 service
- e. Disaster recovery
- f. VOIP Security Issues Relevant to Congressional deliberation to revise the '96 Telecommunications Act

***Tentative Schedule for those wishing to present a paper or participate on a panel:***

Intent to Participate:	April 1, 2005
Papers Due:	April 15, 2005
Notification of Acceptance:	May 15, 2005
Final papers due:	May 25, 2005

Send papers and presentation proposals to  
Ram Dantu or Duminda Wijesekera  
[rdantu@unt.edu](mailto:rdantu@unt.edu)  
[dwijesek@gmu.edu](mailto:dwijesek@gmu.edu)

For logistical and registration information, contact  
Elizabeth Saggese: [esaggese@virtualmgmt.com](mailto:esaggese@virtualmgmt.com),  
<http://pfidc.com/voip>

For program and agenda updates, visit:  
<http://www.csci.unt.edu/~rdantu/2ndVoIPWorkshopProgram.htm>

**Program Committee**

***Technical:***

Dipak Ghosal, UC Davis  
Tim Gibson, DARPA  
Carl Landwehr, NSF  
Mohamad Sharif, GMU  
Barry Sweeney, SAIC  
Timothy Grance, NIST  
Tom Miller, NSA  
Douglas Maughan, DHS  
Sastri Kota, Harris Corporation  
Mike Frendo, Cisco  
Henning Schulzrinne, Columbia University  
Dennis Baron, MIT  
John Larson, Sprint  
Stephen Hillier, Entrust  
Peter Thermos, Telcordia  
Ronald Bonica, Juniper Networks  
Pradeep Samudra, Samsung,  
Manuel Vexler, IPCC

***Law and Policy:***

Paul Kurtz, CSIA  
Emily Frye, CIPP/Touchstone  
Kris Monteith, FCC (invited)  
Roger Cressey, Good Harbor Consulting LLC

**Sponsors:**

**Supporting Organizations:**

