



# IEEE MonAM'2007

5-6 November 2007  
Toulouse, France

## Program

### Monday, November 5th

9h-9h30 **Welcome session**

9h30-10h30 **Invited talk**

Herbert Bos - Vrije Universiteit Amsterdam, NL

***Monitoring for security: promising work and useless techniques***

The threat landscape is changing rapidly and the monitoring tools for yesterday's threats may be rendered irrelevant in the near future. In this talk, Herbert Bos will present a personal perspective on what is needed in monitoring, and which techniques should be considered either promising or obsolete.

10h30-11h **Coffee break**

11h-12h30 **Session 1: Syn flooding**

An efficient online anomalies detection mechanism for high speed networks

*Osman Salem, Sandrine Vaton, Annie Gravey – ENST Bretagne, France*

Enhanced TCP SYN attack detection

*V. Thing, M. Sloman, N. Dulay – Imperial College London, UK*

SYN flooding attack detection by TCP handshake behaviour observation

*M. Bellaïche – école polytechnique de Montréal, Canada, J.C. Grégoire – INRS-EMT, Canada*

12h30-13h30

## **Lunch**

13h30-15h

## **Session 2: Attack detection (1)**

DDoS attacks against PIM-SM control plane

*B. Hilt – university of Haute Alsace, J.J. Pansiot – LSIT, France*

Denial-of-Service flooding detection in anonymity networks

*J. Oberender, M. Volkamer, H. De Meer – university of Passau, Germany*

Building multiple behavioral models for network intrusion identification

*W.Wang, S. Gombault, A. Bsila – GET/ENST Bretagne, France*

15h-15h30

## **Coffee break**

15h30-17h

## **Session 3: Unclassified**

Signature detection in sampled packets

*G. Muenz, N. Weber, G. Carle – university of Tübingen, Germany*

Improving web traffic inference using page level embedding information

*O. Paul – GET/INT, France*

SHARK: Spy Honeypot with Advanced Redirection Kit

*I. Alberdi, E. Alata, V. Nicomette, P. Owezarski, M. Kaaniche – LAAS-CNRS, France*

17h- 18h

## **Short papers session**

Optimal placement of different types of monitoring equipment in transparent optical networks

*M. Kiese, C. Mas Machuca – Munich university of technology, Germany*

Bringing the pieces together: an architecture for network scan mitigation

*E. Le Malécot, Y. Hori, K. Sakurai – Kyushu university, Japan*

An entropy based analysis method of network delays for a discriminating DoS attack detection

*Y. Labit, P. Owezarski – LAAS-CNRS, France*

Monitoring both OS and program level information flows to detect intrusions against network servers

*G. Hiet, L. Mé, B. Morin, V. Viet Triem Tong – Supélec, France*

19h-

Social event

Visit of the Bemberg art collection museum at Hotel d'Assezat

Banquet in the roman basement of hotel d'Assezat

# Tuesday, November 6th

9h-10h30

## Session 4: Attack detection (2)

A collaborative approach for proactive detection of distributed denial of service attacks

*J. François – university Henri Poincaré, France, A. El-Atawy, E. Al Shaer – DePaul university, USA, R. Boutaba – University of Waterloo, Canada*

SQL injection and password guessing detection and mitigation for next generation IMS

*M. Sher – technical university of Berlin, Germany*

Rapid aggregate defence for denial of service attacks

*A. Bitorika, C. Mc Goldrick, M. Huggard – university of Dublin, Trinity College, Ireland*

10h30-11h

## Coffee break

11h-12h30

## Pannel

“Threats for the Internet: what tools for evaluating the actual risk”

Pannelists:

- Vincent Nicomette                      LAAS-CNRS
- Olivier Paul                                INT
- Radu State                                 LORIA

Moderator: Philippe Owezarski              LAAS-CNRS