JOOP BAUTZ INFORMATION SECURITY AWARD
JURY RAPPORT 2012

The Jury of the Joop Bautz Information Security Award 2012 has, after careful consideration, come to the unanimous conclusion that for the Joop Bautz Information Security Award 2012 is nominated:

Sukalp Bhople

for his paper titled:
"Server based DoS vulnerabilities in SSL/TLS Protocols**"**

The Jury is herewith considering the following:

In 2012 it became possible for the eleventh time to nominate candidates for the Joop Bautz Information Security Award, an award established by 3 institutes, active in the field of information security in the Netherlands (PvIB, ISACA and NOREA).
The assessment criteria for the award are the following:

- **Theoretical depth:** resource utilization, depth, approach, presentation, accuracy.
- **Practical relevance:** originality, effectiveness and efficiency, "are we waiting for this?"
- **Renewal:** originality, ease, innovatory
- **Suitability:** social basis, cost factors, scope, acceptance

After studying the total of 9 nominations, the jury has nominated 3 papers: including the recitation of Mr. Bhople. Thereby, the jury is considering the next:

As a user of the web, everyone knows the meaning of the lock-icon (icon for the Secure Sockets Layer "SSL" protocol), usually in the upper right in the browser window. The lock-icon, whether open or not, should give us the confidence that unauthorized third parties, not after great difficulty and effort, can't watch with the multiplicity of transactions people do on the web. Bhople asked himself the question what the impact might be of a different kind of threat, namely the elimination of websites through targeted, massive attacks ("Distributed Denial of Service attacks", in other words: DdoS) on the SSL protocol. After a highly detailed analysis of SSL, the different ways to enable DDOS attacks on SSL, Bhople has found several weaknesses in the current way of using SSL. In particular, the so-called "Handshake" elements, based on intensive cryptographic operations in SSL provides a target, proposes Bhople.

The jury assessed the work piece with the qualification very well on all criteria of the Award. The jury thereby considered that – given the wide distribution of SSL in the web and the social impact of the paralyzing of the web services – Bhople's work is highly relevant and compelling to further study and action. The padlock in the browser shouldn't be the cause of the lock of the web as a whole.

In short, a well-argued paper on a current topic with high social relevance with several innovative insights it is, qualified for the award.

The Jury of the Joop Bautz Information Security Award 2012,

Mr. P. van Dijken (chairman) ing. K.F. Rorive MSc CISSP CISA CISM (secretary)