**09:45** De l'évolution des menaces : à qui la faute ?

*On the evolution of threats: who is faulty?*

**Marc Dacier**, Symantec Research Labs Europe, Sophia Antipolis

November 2nd, 2008, will mark the 20th anniversary of the appearance of the first computer worm able to spread quickly and widely all over the Internet: the Internet worm, also known as the Morris Worm. This is probably a good time to briefly recap the observed evolution of the Internet threats since that date. We will see that the most recent trends seem to indicate the existence of a professional underground market to sell or rent malicious services and tools. In parallel, we will see how solutions have evolved with respect to the arising threats. We will present the classical intrusion detection and prevention systems and position them in the broader context of dependability mechanisms. We will review the problem of assessing the efficiency of these solutions and we will show, based on experimental results, how difficult benchmarking these tools can be. Last, we will try to understand why, twenty years after the Morris Worm, we have apparently failed in solving the Internet security issues. We will conclude by offering avenues for future work as well as perspectives on potential new threats.

**Jeudi 9 octobre**

**Marc Dacier** joined Symantec as the director of Symantec Research Labs Europe in April 2008. From 2002 until 2008, he was a Professor at the Eurecom Institute, France. From 1996 until 2002, he worked at IBM Research as the manager of the Global Security Analysis Lab. (GSAL). He obtained an IBM Outstanding Technical Achievement Award for his contribution to the business of IBM Global Services. Also, the GSAL team pursued several projects in the intrusion detection domain which led to the creation of the Tivoli Risk Manager product.

In 1995, he worked within France Telecom as an external consultant in charge of security for the organization responsible for the strategy of the IT infrastructure. From 1992 until 1994, he was a member of the Dependability group, at LAAS-CNRS, working on quantitative evaluation of operational computer security and obtained his PhD there from the Toulouse National Polytechnic Institute. From 1989 until 1991, he was with the University of Louvain.

Since 1997, he has been giving, as an invited researcher, an intrusion detection seminar at the University of Louvain (UCL), Namur (FUNDP) and Liège (ULG) and also at the ENSEEIHT in Toulouse. In 2002, he has received the title of invited professor at UCL and associate professor at ULG.

In 1998, he co-founded with K. Jackson the "Recent Advances on Intrusion Detection" Symposium (RAID). He is now chairing its steering committee. He has served in more than 60 program committees of major security and dependability conferences and is a member of the steering committee of the "European Symposium on Research for Computer Security" (ESORICS).

He was a member of the editorial board of the following journals: IEEE TDSC, ACM TISSEC and JIAS.