

## CALL FOR PAPERS

# The 1st International Workshop on Middleware Security (MidSec 2008)

December 2, 2008  
Leuven, Belgium

Co-located with the 9th ACM/IFIP/USENIX International Middleware Conference  
(MIDDLEWARE 2008)

Modern applications are more and more predominantly built around distributed programming paradigms. Event-based systems, mobile agent frameworks, peer-to-peer networks, grid computing, and Web service applications are examples of architectures that are used by a large share of the present software base. These paradigms expose applications to new, ever-growing security threats. For this reason, middleware platforms have always been mindful about offering out-of-the-box security services like communication encryption, user authentication, and access control. Such features are now considered commodities in many middleware platforms, e.g., CORBA, Java EE, and .NET. However, focused research is still necessary to address advanced areas of security. Examples are identity management, privacy and anonymity, accountability, application protection, and so on.

The *goal* of this workshop is to provide a venue for the security and the middleware communities to collaborate and create new momentum for the topic area.

Original submissions are welcome from both academic and industry experts. The *topics of interest* include, but are not limited to:

- Middleware security: middleware software is an asset on its own and has to be protected.
- Security co-design: trade-off and co-design between application-based and middleware-based security.
- Context-sensitive security middleware: advanced security services and features offered by the middleware layer to pervasive and situated systems.
- Policy-based management: innovative support for policy-based definition and enforcement of security concerns.
- Security features: interaction between security-specific and other middleware features, e.g., context-awareness.
- Advanced identification and authentication mechanisms: e.g., means to capture application-specific constraints in defining and enforcing access control rules.
- Availability: protection of availability of middleware services.
- Security in agent-based platforms: protection for mobile code and platforms.
- Security in aspect-based middleware: mechanisms for isolating and enforcing security aspects.
- Middleware-oriented security patterns: identification of patterns for sound, reusable security.
- Middleware-level security monitoring and measurement: metrics and mechanisms for quantification and evaluation of security enforced by the middleware.

### Important dates

Paper submission due: August 1, 2008  
Acceptance notification: September 15, 2008  
Camera-ready papers due: October 8, 2008

## Submission guidelines

The workshop solicits original research papers in any of the above-mentioned topics. The workshop organizers also solicit relevant experience results from industry experts. Preliminary research results can be submitted in the form of short papers.

Full papers should not exceed *6 pages* and should be prepared according to the standard ACM format (<http://www.acm.org/sigs/publications/proceedings-templates>). Short papers should be limited to *3 pages*.

Accepted papers will be published in the workshop proceedings and made available through the *ACM Digital Library*.

## Organizers

*Riccardo Scandariato*, Katholieke Universiteit Leuven (BE)  
*Giovanni Russello*, Imperial College London (UK)

## Program committee

*Jean Bacon*, University of Cambridge (UK)  
*Konstantin Beznosov*, University of British Columbia (CA)  
*David Chadwick*, University of Kent (UK)  
*Bart De Win*, Katholieke Universiteit Leuven (BE)  
*Naranker Dulay*, Imperial College London (UK)  
*David Eyers*, University of Cambridge (UK)  
*Fabio Martinelli*, CNR (IT)  
*Anand Ranganathan*, IBM (USA)  
*Brian Shand*, University of Cambridge (UK)  
*Tine Verhanneman*, Atos Worldline (BE)  
*Ian Welch*, Victoria University of Wellington (NZ)