The term “ambient intelligence” (AmI for short) is used to identify an ambitious vision in which technological developments that will enable heterogeneous networked systems and devices with different computing capabilities to cooperate in response to recognition of everyday life activities of people, in order to support them carrying out these activities.

In February 2001, the IST Advisory Group (ISTAG) published a visionary report on the scenarios for Ambient Intelligence in 2010. Ten years after its publication and one after its target date, we have seen numerous research initiatives that have produced significant advances, but we are still far from that vision. One of the key issues to consider when thinking about a future in which we will live surrounded by Ambient Intelligence systems is security. No matter how fascinating and useful AmI systems may be, the fact is that the lack of appropriate security mechanisms will hinder the adoption of those systems. Therefore, a key prerequisite for the realization of this vision is the secure and dependable interaction of the different components and devices of ambient intelligence systems in all contexts where it can take place.

In this scenario, the concepts of “system” and “application” as we know them today will disappear. Applications in AmI environments will evolve from well-defined pieces of software, with static architectures, well-defined limits and owners, to what we could call AmI ecosystems, lacking a fixed architecture, controlled limits and even owners. The simple trust models in which current security solutions are based will not be appropriate anymore in these ecosystems. Given the nature of these environments and the needs for scalability, context awareness and dynamic reaction, the only feasible model will be considering the eco-system as a “complex self-organising system”.

Therefore, security solutions for these environments must cope with the combination of heterogeneity, mobility, dynamism, context adaptation, sheer number of devices, and lack of control over some necessary pieces of software, communication infrastructures and hardware devices by means of a change of paradigm in which security is not anymore based on simple pre-defined trust relationships and assumptions about control of the system or its components.

The focus of this special issue will be on the security models, protocols, infrastructures or solutions addressing the security, privacy, trust and dependability aspects of AmI.
Topics of interest of this Special Issue include, but are not limited to:

- Security, privacy, trust and dependability aspects of AmI
- Security and trust in complex self-organising systems;
- Dynamic local feedback control for system security;
- Security and emergent behaviour;
- Self-learning for security and trust;
- Security engineering for AmI;
- Device, infrastructure and software components evolution in AmI;
- Trust models for highly distributed systems;
- Surveillance mechanisms for AmI environments;
- Contextualised and hybrid diagnosis of faults and attacks in AmI environments;
- Fault tolerance and resilience;
- Human centred evaluation of security, privacy and trust;
- Human-meaningful security and privacy interfacing for future computing ecosystems;
- Benchmarks for evaluation of AmI environments.

Online Submission

Authors should submit their manuscripts online. Electronic submission substantially reduces the editorial processing and reviewing times and shortens overall publication times. From the journal webpage at:

https://www.editorialmanager.com/aihc/

Please click on 'Submit a manuscript'. Here you will find the label 'SDAMI' then you can upload all of your manuscript files following the instructions given on the screen.

<table>
<thead>
<tr>
<th>Editor-in-Chief</th>
<th>Guest Editor</th>
<th>Guest Editor</th>
<th>Guest Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vincenzo Loia</td>
<td>Antonio Maña</td>
<td>Jacques Bus</td>
<td>George Spanoudakis</td>
</tr>
<tr>
<td>University of Salerno, Dept. of Mathematics and Informatics, Salerno, Italy</td>
<td>University of Málaga, Computer Science Dept., Málaga, Spain</td>
<td>DigiTrust.EU, The Netherlands</td>
<td>City University London, Dept. of Computing, London, UK</td>
</tr>
<tr>
<td><a href="mailto:loia@unisa.it">loia@unisa.it</a></td>
<td><a href="mailto:amg@lcc.uma.es">amg@lcc.uma.es</a></td>
<td><a href="mailto:jb@digitrust.eu">jb@digitrust.eu</a></td>
<td><a href="mailto:gespan@soi.city.ac.uk">gespan@soi.city.ac.uk</a></td>
</tr>
</tbody>
</table>

**Tentative timetable**

<table>
<thead>
<tr>
<th>Deadline for manuscript submissions</th>
<th>Information about manuscript acceptance</th>
<th>Expected publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 1, 2012</td>
<td>June 1, 2012</td>
<td>Fall, 2012</td>
</tr>
</tbody>
</table>