

Submission to NEM for Security Cluster

Detailed Cluster Description

Cluster title: NEM Security Cluster

Acronym (optional): NEM SEC

Name and e-mail address of Cluster Leader: James Clarke, jclarke@tssg.org

Name and e-mail address of a Cluster co-Leader (optional): Jimmy McGibney, jmcgibney@tssg.org

The NEM Technology Platform is addressing the architectures central to the convergence of telephony and voice services, Internet and data services, and home media. This has a pivotal role in the EU IST FP7 strategy and is important to a range of overlapping academic and industrial interests. In addition, it will be an explosive growth area with the move from physical media to on-line media content creation and provision. In order to succeed, major issues, concerns and challenges in relation to Trust, Security and Dependability (TSD) will need to be addressed and, thus, there will need to be significant research and development of TSD areas across many disciplines within the Networked and Electronic Media domains.

The SRA¹ identifies five big challenges on which NEM is focusing these include:

- a) To create interoperable network infrastructures that enable seamless multimedia networking
- b) To empower end-users by putting the user first
- c) To promote “electronic content from all to all”
- d) To merge the various media and content formats
- e) To develop new middleware for media applications

Transversal to these challenges are a large number of Trust, Security and Dependability challenges, some of which were already identified at a number of recent TSD Workshops organised by SecurIST² and ESFORS³ co-ordination actions. For example, where NEM identified a focus on challenge b) above can be linked with figure 1 below, which illustrates the challenges discussed at a recent ESFORS workshop. Both areas are concerned with end-user impact. Thus, this Security Cluster within the NEM framework can explore opportunities to integrate these common research challenges and efforts.

¹ <http://www.nem-initiative.org/Documents/NEM-BC-001.pdf>

² www.securitytaskforce.eu

³ www.esfors.org

	Stream A Secure applications & Security Services	Stream B Secure Service Ecosvstems	Stream C Stakeholders expectations
Security Engineering	Trusted Core Formal methods	Predictability Contextual Engineering	Security cost
Dependability Engineering	Privacy in infrastr. Identity at cross-X	SOA intrusion Self-healing	Certification Liability/legal
Analysis, Control, Monitorin	High level policy Virtualization and isolation	S-Negotiation Cooperative enforcement	Metrics Emerging risks

Figure 1: Challenges identified at ESFORS Joint Workshop on Software and Services Development, Security & Dependability, Paris, 6-7th September, 2006.

Additional major challenges identified within workshops held by the TSD community relevant to NEM activities include:

- **Unified approach for an Interoperable Digital Rights Management (DRM) environment.** There was consensus regarding a need for an EU-based approach for digital rights management to enable the EU to become a more effective content creation and provision environment.
- **Safe and secure software download enabling networks and device re-configurability.** Dependability issues in safe/secure downloads must be addressed. Some of the issues include intelligent function firewalls, intelligent access controls, need for user friendly download and building up of software trust and risk awareness.
- **Development of secure Secure data management, and synchronization and private exchange of user profile and context information.** One of the future challenges for FP7 is a paradigm shift of gradually replacing the physical boundaries with logical boundaries maintaining context in order to move from a system-centric, or “Central Command and Control” to a Citizen centric, or “Empowerment of the Citizen! Approach to security.
- **Development of secure and robust watermarking algorithms.** Digital watermarking, i.e. the possibility of imperceptibly and indissolubly attaching a piece of information to a hosting digital asset such as a video, a still image or an audio file, has been proposed as a viable solution to several security problems related to the way digital assets are handled in our digital age. The addressed problems include ownership verification, copyright protection, tracing of illegal uses and/or non-allowed redistribution etc..
- **Asset authentication through intrusive (watermarking) and non intrusive (digital forensics) techniques.** Authentication of digital data has been traditionally addressed by means of cryptographic primitives, such as digital signatures and hashing. Such techniques, though, guarantee the perfect integrity of electronic documents since authentication fails if even a single bit is altered. Such a strict definition of authenticity is not always appropriate for multimedia data where there is an interest in permitting some alterations that retain the perceptual meaning of the original content.

- **Conditional access to the digital assets.** Another essential ingredient of any secure asset management system is the possibility of restricting the access to the digital assets, or part of them, to authorized users. Whereas cryptographic techniques are an obvious solution, the interplay of encryption and signal processing must be carefully considered. In order to allow a secure, fast, and flexible access to the digital assets, it is in fact fundamental that the cryptographic primitives are adapted to, or, even better, jointly designed with the asset format.
- **Asset processing in the encrypted domain.** The availability of signal processing algorithms that work directly on encrypted data would be an invaluable help for application scenarios where “valuable” signals must be produced, processed or exchanged in digital format.
- **Covert Communications (steganography and steganalysis).** Another key issue is the possibility of establishing a covert communication channel by means of steganographic tools.

This list is not an exhaustive list of the common challenges that the TSD and NEM communities must address. The function of the NEM SEC cluster will be to bring together the wider community in the TSD and NEM areas to further elaborate important R&D challenges that need to be addressed and leverage existing efforts to address these challenges in a structured, collaborative environment and raise their awareness to the wider NEM platform participants.