STORM - Collaborative Security Management Environment

Theodoros Ntouskas, George Pentafronimos, Spyros Papastergiou

STORM - Collaborative Security management environment

Theodoros Ntouskas, George Pentafronimos and Spyros Papastergiou

Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 185 34 Piraeus, Greece,
{tdouskas,gpentas,paps}@unipi.gr

Abstract. Security Management is a necessary process in order to obtain an accurate security policy for Information and Communication Systems (ICS). Organizations spend a lot of money and time to implement their security policy. Existing risk assessment, business continuity and security management tools are unable to meet the growing needs of the current, distributed, complex IS and their critical data and services. Identifying these weaknesses and exploiting advanced open-source technologies and interactive software tools, we propose a secure, collaborative environment (STORM) for the security management of ICS's.

Keywords: Security Management, Risk Management, Vulnerability Assessment tools, Security Tools, Collaboration

1 Introduction

The most critical and sensitive data of the organizations is hosted in their Information and Communication Systems (ICS). Degradation, interruption or impairment of their ICS has serious consequences on safety, loss of sensitive data, loss of reputation or loss of service making security management one of the most important organizational concerns [2]. Current ICSs are distributed; complex and multidimensional resulting to the fact that security management is a cooperative obligation requiring the involvement and participation of all ICS participants.

Existing security management (e.g. ISO-15408 [31], ISO-17799 [32], ISO-27001 [33], ISO-27002 [34]) and risk assessment (e.g. Cobra [12], CRAMM [13], EBIOS [17]) tools do not enable collaboration and they do not consider all aspects (technological, business, legal, economical) that influence the evaluation of the ICS threats and vulnerabilities leading to incomplete and ineffective security management, with generic security policies and incomplete security procedures.

The risk management for current complex organizations (e.g. large-scale infrastructures, critical infrastructures, large enterprises) requires many interviews with all participants in order to identify the architecture of the ICS, the assets, and their interdependency, risks and criticality (from an organizational, technological, legal, business and economical perspective).

Furthermore, it does not exist an automated collaborative tool embedding security standards, methodologies, tools and guidelines that continuously guide and train the participants in the security management in order to:

- Perform risk assessment for risk identification
- Conduct vulnerability assessment
- Execute penetration tests/scenarios
- Implement appropriate countermeasures
- Design security policy and procedures
- Design security business continuity and disaster recovery plans

The aim of this paper is to contribute to the above challenge by providing a collaborative security management tool (STORM) which provides:

- **Innovative collection of security knowledge.** Using the STORM environment the necessary information will be collected from all participants, minimizing the gathering time, reducing costs for the organizations and most importantly taking into account the security knowledge of all participants of the ICS in order to obtain an accurate security policy.
- **Secure dependable and collaborative environment**. By the use of STORM modules, the governance of complex organizations will be able to establish and maintain a secure cooperate environment for their local and external users.

STORM is a prototype of a new generation, collaborative, innovative security management environment, which will be able to provide the necessary level of confidentiality, reliability, interactivity and interoperability of the organizations and their ICS's. The proposed STORM environment is an open and cost effective approach that is based on widely used collaborative web 2.0 technologies such as wikis, blogs, RSS and forums.

The rest of the paper is organized as follows: Section 2 describes existing standards and methodologies for Security Management and analyzes the ICS complexity. Section 3, describes the STORM architecture and its basic components. Finally, Section 4 draws conclusions.

2 State of the art

Security Management is a continuous and systematic process of identifying, analyzing, handling, reporting and monitoring operational risks of an organization [6][18]. Security Management is an important governance and administration procedure aiming at the protection of an organization from internal and external risks that would negatively affect the achievement of its operational objectives.

Current ICS's are characterized by growing complexity, distribution of their Information System (IS) (network, hardware, software, human resources) in various locations (rooms/buildings/cities) and by the plethora of electronic services. In addition, these complex ICS's interact, interwork and their business become dependent on other organizations (e.g. providers, partners, banks, insurance companies, Tax authorities). They have a large number of users (internal, external administrators, users, providers), and they face a growing number of different types of spatial and temporal dispersion effects of attacks.

Despite the growing need for effective security management within the organizations, the existing security-related methodologies, standards and frameworks are inadequate to meet the above needs of current ICS in a holistic and integrated way. More specifically:

- Existing security management standards/frameworks/methodologies for the establishment of corporate security governance (e.g Cobit [11], ITIL [10], ValIT [56], ISO-17799 [32], ISO-27001 [33], ISO-27002 [34]), have not been implemented in a tool since they present specific limitations. They usually define principles and provide only guidelines mostly in the form of recommendations rather than strict rules that should be followed.
- Existing risk management methodologies (i.e. Cramm [13], Octave [43], ISO-15408 [31]) and their automated tools (e.g. Cramm [13], Cobra [12]) are costly, they require numerous and time consuming face-to-face interviews with all the administrators, not allowing collaboration, resulting to the insufficient collection of all available security knowledge of all participants.
- Most of available methodologies and frameworks for security testing [4], [52], [60], [50], [46], [25], [8] describe test cases and they indicate tools that can be used in each test providing merely a description of their capabilities. Nevertheless, the tracing and the correct configuration of the required vulnerability assessment tools is a time consuming process which requires specific expertise. Therefore, there is a need for consolidated vulnerability assessment information pertaining to the proper configuration and installation of the VA tools as well as the provision of an integrated VA environment that offers a comprehensive and large collection of security-related tools.
- Disaster Recovery and Business Continuity standards (i.e. BS 25999-1 [9], BCI GPG [7], ITIL V3 [10], HB 292 -2006 [24]) are unable to meet the needs of the current distributed IS's since they have not been implemented in an automated tool.
- The renewal, updating and awareness of these security documents (security policy, Disaster Recovery and Business Continuity plans) is done manually every time something changes in the ICS or in the security procedures which are costly and time consuming processes requiring a variety of organizational resources.

Therefore, there is an imperative need for continuous, collaborative, holistic and effective security management of the ICS. The proposed STORM environment, described in the following sections is an open, cost-effective, collaborative approach to security management.

3 STORM collaborative environment

Because of the changing conditions under which an organization operates today (distributed, complex and diverse technological environment, globalization, economic crisis), the implementation and maintenance of an accepted level of ICS security is requiring a planned and organized task. STORM contributes

to the creation, enhancement, monitoring and assessment of the security of the information and communication systems providing an innovative, interactive collaborative environment that encompasses a bundle of primitive services which allow the organization to:

- identify and depict the ICS infrastructure;
- identify the applying security policies, procedures, standards and guidelines;
- specify, evaluate and classify daily risks and threats of the ICS continuously collecting the security knowledge of all operational ICS participants (administrators, users, providers);
- recognize the impacts (business, economical, technological, legal) of upcoming incidents on the operations of the ICS;
- execute technical vulnerability assessment with live scenarios (based on accepted vulnerability assessment methodologies and techniques) identifying at real time the security needs of the ICS;
- select reliable and appropriate countermeasures to achieve the confidentiality, availability and integrity of data;
- on-line generation/formulation/monitor/renew/update all the security documents (security policy, Business Continuity and Disaster Recovery Plans);
- continuously monitor new laws, standards and best practices.

In order to achieve these, the STORM collaborative environment is composed of four layers as depicted in the following Figure.

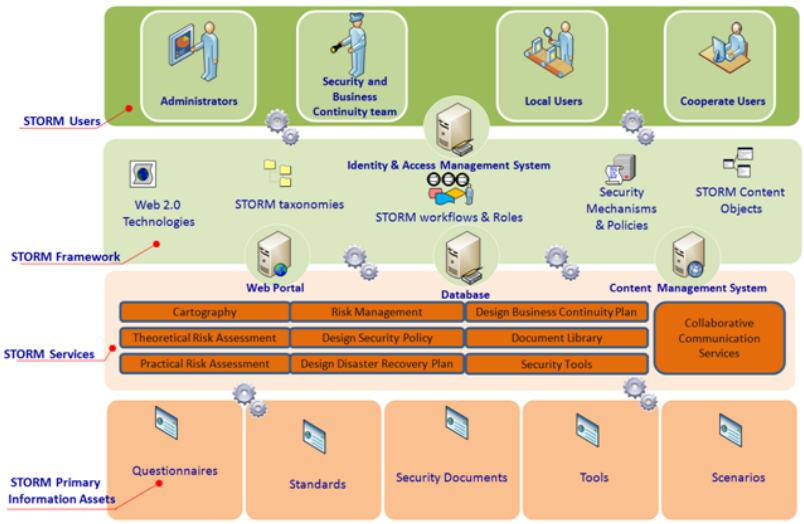

Fig. 1. STORM collaborative environment

STORM architecture, its basic components and their functionalities, are described in the following sections.

3.1 STORM Architecture and Services

STORM aims to become the harbinger of a new generation security management tool for ICS, stimulating the collaboration among all stakeholders. Figure 1 depicts the proposed architecture that encompasses the core participants and entities distributed in four distinct layers as follows:

Layer 1 - STORM Users: This first layer consists of the four groups of users namely, Security and Business Continuity Team, Administrators, local Users, external users. Considering the fact that local and cooperate users may not perceive critical security factors (e.g. threats, vulnerabilities, impacts) the same way as security experts, different access privileges to the STORM services have been applied to the aforementioned user groups. Remarkably, only the members of the Security and Business Continuity Team are responsible for properly and adequately providing initial content to the system and specifically all the primary information assets comprised at Layer 2 of its architecture, that are necessary for harmonizing security management procedures.

Layer 2 - The STORM Framework: The main components and the individual systems that comprise the core STORM environment.

Layer 3 - STORM Services: At this layer, an integrated bundle of security services is provided that aids the organization to apply an accurate, reliable and flawless corporate security management of ICS.

Layer 4 - STORM Primary Information Assets: All related standards, methodologies, best practices, related legislation are the assets of the STORM; typical examples are: Business Continuity and Disaster Recovery Standards, Security Management Standards methodologies, Risk Analysis questionnaires, Vulnerabilities scenarios, Security Policy, Disaster recovery/Business Continuity plans, Disaster Scenarios. These assets are structured documents in STORM Document Library.

3.2 Layer 1 - STORM Users

The STORM participants as described in Layer 1 are the following:

- The administrators of the IS who continuously inform the collaborative tool with all the necessary information (technical instructions, manuals, samples of business continuity and disaster recovery plans, international standards, best practices, open source security tools and scenarios etc.), create the questionnaires and the necessary recovery forms, define the responsibilities of users, control and renew the lists of the installed software and hardware of the information system.
- The members of the security and business continuity team, make an assessment of the criticality of services, analysis and evaluation of risks, risk management using appropriate countermeasures and implement all the procedures of the security policy. They are able to continuously be informed with the new standards and best practices and apply them directly on the system.

- Local users of information systems (e.g. accounting user etc) will be able to actively participate in the collaborative security process, find information on technical and security procedures and as a result any difficulties may be treated effectively. Also they will be trained/informed about all the security procedures through the STORM communication module (with wiki/forum/polls).
- Cooperate users which cooperate with the organizations (e.g. custom offices, banks, agencies, suppliers, service providers, other organizations) can be informed about security rules and conditions for safe interconnection and access to the information systems of the organizations. In this way there will be safeguards put in place, minimization of threats, and trust in the quality of services.

3.3 Layer 2 - The STORM Framework

The STORM framework consists of two central entities. The fist is the Identity and Access Management (IAM) System which properly specifies and enforces security and privacy policies, used to control access to STORM services. IAM incorporates security mechanisms and policies that enhance the STORM platform with proper authentication and authorization properties and Single-Sign-On (SSO) procedures, enclosing end-user's preferences and requirements. Based on the above procedures, different user roles (administrators, local users etc.) have access to specific STORM services according to their business needs and requirements. This component is based on open source Open SSO [44].

The second major entity of the framework is STORM System that is comprised of the following components:

- **Web portal:** A Web Interactive System, which provides secure access to security related information and content, retrieved and processed from diverse sources, in a unified and user-friendly way. This system is based on collaborative Web 2.0 technologies and automated, open, interactive and reliable technological tools (such as collaborative forums, blogs, Wikis etc.). The STORM system will actually provide a consistent look and feel with secure access control and procedures for the integrated applications of the project. The STORM Web portal will serve as a unified secure access and presentation point to the full range of security services.
- **Enterprise Service Bus (ESB):** ESB is essentially a lightweight messaging framework integrating different technologies, devices and data transfer protocols, ensuring that different systems and applications communicate through a common channel to exchange information with other organizations.
- **Business Process Modelling (BPM):** It undertakes the responsibility to monitor, manage, analyze and implement the business logic of complex and distributed workflows of the services provided by the STORM system.
- **Decision Support System (DSS):** DSS facilitates the combination of a set of information in order to solve problems and reach tactical and strategic

decisions in several security and privacy issues. These decisions can be considered more in the form of suggestions and recommendations rather than strict injunctions that should be followed. The users will be able to modify, complete, or refine these decision suggestions according to their needs. Representative example is the definition of a security and privacy risk mitigation strategy taking into consideration the enterprise financial status and the applied countermeasures.

- **Ontologies and Semantic Structures (Knowledge Base):** A collection of semantic structures (notably ontologies/taxonomies) modelling the STORM content as well as their semantic relationships will be designed, implemented and integrated within the STORM system. Thematic, security and privacy related ontologies/taxonomies will be defined to better organize the various quantities of the assets stored in the repository. These will bring context to words, topic areas and search results, providing a hierarchical structure of asset categories, from general to specific. We conveniently call the set of semantic structures of the STORM system, as the STORM Knowledge Base.
- **Content Management System (CMS)** responsible for creating, editing, management and publication of all the primary and processed content in a consistent and structured way. It consists of:
  – advanced content management tools (e.g. rich text editors, live page editing and scheduling, and advanced document managers) in order to provide the STORM friendly environment;
  – intuitive front end user interfaces that share a set of common characteristics to promote user friendliness and accessibility;
  – functionality for collecting, organizing and managing content from multiple sources (e.g., databases, repositories) and multiple formats;
  – STORM taxonomies for better access to the STORM primary assets and content.
- **STORM Repository:** All STORM primary assets (all related standards, methodologies, best practices, legislation, Risk Analysis questionnaires, Security Policy, Disaster recovery/Business Continuity plans) are stored in a repository.

All the aforementioned elements are the backbone infrastructure of the STORM framework. They will be combined in an effective way to establish a highly agile automation Services Oriented Architecture (SOA) environment that can boost both re-engineering and the integration of a set of security and privacy related services that will be described in the following section.

3.4 Layer 3 - STORM Services

The services offered by STORM (Layer3) are depicted at the figure 2 and described in detail as follows:

Cartography module: The main objective of this module is to describe critical information and communication systems in order to depict all their security-related aspects. These aspects are not confined only to technical issues, but they

are also concerned with the business processes in which the systems are embedded. In order to describe the information and communication systems, STORM has adopted and integrated an object modeling approach based on the ISO Reference Model for Open Distributed Processing systems (RM-ODP) [57] standard in combination with the Unified Modeling Language (UML). The RM-ODP offers a general framework and a reference model based on five different viewpoints that identifies the crucial characteristics that qualify the systems while the UML provides the notation for representing the identified features.

The five viewpoints as described by RM-ODP and adopted by STORM are the following:

- *Enterprise viewpoint.* A viewpoint of the system and its environment that focuses on the technical guidelines and policies associated with the system as well as the system's purpose of operation, scope and business requirements. Also, it deals with aspects of the enterprise such as its organizational structure, which affect the system.
- *Information viewpoint.* A viewpoint which specifies and describes the information structure of the system. Specifically, it focuses on the information that is stored, processed and exchanged in the system.
- *Computational viewpoint.* A viewpoint which focuses on functional decomposition of the system into objects which interact at interfaces.
- *Engineering viewpoint.* A viewpoint which describes the way different objects of the system interact with each other as well as the resources required for this communication.
- *Technology viewpoint.* A viewpoint which focuses on the individual hardware and software components which compose the system.

The proper and accurate analysis and representation of the information and communication systems aid the early discovery of security vulnerabilities, inconsistencies and redundancies in these systems.

Theoretical Risk Assessment Module: providing the following functionality:

- *Online Forms* for user identification (responsibilities, roles etc.), asset identification (servers, routers, switches, applications, databases etc), reporting of their interdependencies with other systems, description of applications, detailed record of operational procedures.
- *Collaborative Questionnaires.* Embedded online questionnaires for the accomplishment of:
  - IT assets (software and hardware) identification
  - impacts determination (based on various security scenarios related to availability, integrity and confidentiality loss),
  - threats, vulnerabilities and risk identification.

The posted questionnaires are filled in by all participants and are collected and analyzed by the corresponding users through charts .The participants, answering the questionnaires, will be able to give their knowledge from their own

perspective (e.g. deficiencies, security incidents, backup procedures, countermeasures of their department). This allows the accumulation of objective information that can be used as input for the execution of the risk analysis and risk management procedures in an effective and efficient manner.

Fig. 2. STORM Security Management Services

Vulnerability (Practical Risk) Assessment module: This module consists of the following three subcomponents:

1. *Methodologies repository.* An inventory of the most wide-used and accepted vulnerability assessment (VA) methodologies and frameworks (i.e. OWASP [4], OWASP Code review [52], NIST SP800-42 [60], Special Publication 800-115 [50], Penetration Testing Framework (PTF) [46], OSSTMM [25], ISSAF [8])defined and released by the standardization bodies and the research communities. This acts as a reference point of existing methods for network and web application security testing and assessment as well as for forensics analysis.
2. *Tools Repository.* An inventory of open source and freeware tools that can be used in combination with the VA methodologies and frameworks for the deployment of specific security tests. A set of tools-related information concerning installation guides for various operating systems, links to sources codes and executable files as well as expert notifications about capabilities, problems and limitations is also provided.
   Within STORM, the VA tools are divided in the following categories taking into account the provided functionality:
   - Reconnaissance and Discovery: information gathering from publicly available sources and online databases such as IP registries, DNS information, public web sites and search engines (e.g. Dnsmap [15], DNSPredict [16], Fierce [22], Metagoofil [39], Gooscan [23]).

- Network Mapping: acquisition of detailed information about the targets (e.g. Hping3 [27],Nmap [41], TCPtraceroute [54], P0f [47], Zenmap [62], Httprint [28]).
- Vulnerability Identification: discovery and enumeration of candidate vulnerabilities of the examined systems (e.g. OpenVas [45], W3AF [59], Nessus [40]).
- Penetration/Exploitation: exploitation of specific vulnerabilities aiming at gaining unauthorized access to the target systems (e.g. MEF [38], ExploitDB [21]).
- Privilege Escalation: gaining privileged access to the compromised systems (e.g. Hydra [29], [35], Medusa [37]).
- Further Enumeration: discovery of further information (e.g. passwords, network mapping) (e.g. EtterCap [20], Wireshark [61])
- Maintaining Access: establishment of covert channels, back door installation and deployment of rootkits (e.g 3proxy [1], ProxyTunnel [48], TinyProxy [55]).Digital Forensics Analysis: preservation and analysis of digital evidence (e.g. Autopsy [5], [14], Sleuth [51], Volatility [58]).

In addition, a VA environment (VA platform) has been configured and is available in STORM providing a user-friendly access to a comprehensive and large collection of security-related tools ranging from sniffers and traffic analyzer to web scanner and WEP/WPA cracking. The preconfigured environment is a Linux distribution based on Debian 5 that is available as a Live DVD. This allows the potential users either to boot the platform directly from any portable media or to install it to the hard disk or even to run it as a virtual machine. Configuration guidelines of the platform are also available strengthening the trust of the potential users. The main aim of this inventory is to assist individuals and organizations to establish a well-defined security "laboratory" environment enabling them to perform self-assessment in order to improve the security level of their infrastructure.

3. *Lesson Learned Repository.* This component acts as an inventory of common attacks. Its main objective is to bring into focus some of the theoretical and practical concerns of the most common threats. In this context, a comprehensive description of a set of attacks is provided covering all their aspects including exploitable security flaws, applied scenarios, tools which can be used, as well as mitigation recommendations and countermeasures that can be adopted. The attacks have been categorized as follows:
   - Network Attacks: include any methods, processes or means used to maliciously attempt to compromise the security of a network. Representative examples of this type are Distributed Denial of Services attacks, Spoofing attacks, Eavesdropping etc.
   - Application Attacks: include any methods, processes or means used to maliciously attempt to compromise the security of an application. Injection (e.g. sql, soap, ldap), Cross-Site Scripting (XSS), Buffer Overflow attacks are examples of this type.

   In addition, a number of case studies that can be considered as lesson learned can be provided in STORM. These are more in the form of challenges rather

than strict rules that must be followed. The challenges are discriminated in two types. The first concerns case studies of attacks' deployment (e.g. Distribution Denial of Service (DDoS), Denial of Service (DoS)) aiming at the evaluation and validation of the security controls and countermeasures that are integrated in an infrastructure. The impact of the attacks on the target is calculated and recorded in the system as it has to be the prime consideration for further investigation. The second type of case studies gives the opportunity to the potential users (individuals and organization) to analyze the attacks and post their findings in STORM CMS. The challenges concern a wide range of forensic issues such as the detection and analysis of suspicious software/malware, hash analysis, image analysis, partition recovery, signature analysis, file header reconstruction, password recovery, registry analysis, steganography and encryption. Furthermore, the results of case studies conducted within the activities of a set of national initiatives such as HONEYNET [26], CERT Exercises Handbook [19] can be also analyzed and presented in depth in the system. In this way, the users learn not only about the threats, but also how to deploy and analyze them.

Risk Management module: This module via online forms and library aid the organization for the selection of the appropriate taking into account the result of the risk assessment procedure. All participants will be able to give their opinion by using the communication module and agree or propose their new countermeasures.

S**ecurity Policy Module:** This module provides the appropriate functionality for the design and creation of the security policy of the organization using the collaborative forms that are embedded in this STORM module. In addition, all the information related to security policies, procedures, guidelines, rules and responsibilities and credentials at the information and communication systems and services are also available and accessible by all the corporate users via this module.

Administrators and security team will edit and update this module so all the other users of the organization will be able to find information about the security procedures, rules and their responsibilities and credentials at the applications and services.

Disaster Recovery (DR) / Business Continuity (BC) Module: The aim of this module is to provide the functionality required for the design and creation of BC and DR plans. It also contains all the disaster recovery procedures and relevant information such as responsibilities and contact information that are necessary in case of disaster or an emergency event. Further, the module provides forms for building of possible disaster scenarios and for real time responsibilities assignment. More detailed, there have been implemented forms for:

- user responsibilities,
- contact details,
- supplier contact details,
- incident report,
- incident handling,

– recovery procedures,
– backup infrastructure and procedures

Collaborative Communication Services: Provision of a group of communication services.

– Forum for exchanging ideas about security topics or reach consensus on evaluation of risks. This will help all participants to find quickly solutions about daily security or other problems so they will solve their difficulties quick. Also they will be able to discuss about security problems, accept or not the proposed countermeasures or recommend their security safeguards.
– Polls so users will be able to discuss critical security issues allowing them to reach solutions in a collaborative, cost and time effective manner.
– Wiki, based on which, all users will be able to find or propose their own solutions regarding security issues or find details about risk assessment, risk management and vulnerability and the security policy of their organization, so they will be able to solve any difficulty directly.
– Interactive user screens which are used for collaborative risk management and for reporting protection measures.

3.5 Layer 4 - STORM Primary Information Assets

STORM users will be able to perform various actions depending of their roles e.g. local and cooperate users will be able to access the STORM assets which support the STORM services as described in Section 3.4. In particular the following assets will be included: the cartography analysis report of the organization as produced in the Cartography module; the risk assessment questionnaires provided by the Theoretical risk assessment module; all the security related information pertaining to the technical vulnerability assessment (VA) i.e. methodologies, open source and freeware VA tools, installation guides, VA scenarios, case studies; the countermeasures proposed by the Risk management module; security corporate documentation i.e. security policies, Disaster recovery, Business continuity Plans as generated by the Security Policy and the DR/BC modules respectively.

4 Implementation

The development and integration of the main components of the STORM framework is based on the innovative integration of mature technological solutions and tools as follows:

– *Social Networking Tool:* A social networking open source solution that is based on Symfony Framework [53] has been adopted and integrated in the STORM system. This solution is an open source software platform available for social networking that provides a number of Web2.0 components such as, Document Library, Team Calendar, Wikis, Blogs, Forums (Message Boards), Private Site and separate secured areas, Instant Messaging, Announcements & Alerts and Email.

- *Content Management System:* The management of the content, documents, files, information and data related to the security services provided by the STORM system is performed by a CMS solution based on the Symfony Framework [53].
- *Business Process Management (BPM):* A holistic business process management tool, ADONIS [3], has been adopted for the composition of an integrated SOA environment. The tool utilizes notations like Business Process Execution Language (BPEL) standards in order to enable modelling, composition and deployment of service workflows. This tool is also be used in order to implement the Decision Support System that shall be integrated in the system.
- *SOA Environment:* An open SOA strategy has been adopted based on XML technologies and web services-based standards and will be followed for the design, development and implementation of the STORM system. For the integration of the middleware infrastructure [36] (i.e. application servers, enterprise service bus) an Open Source Enterprise Server, has been deployed that hosts the SOA environment.
- *Identity Management System (IMS):* The STORM framework has incorporated a solution, Open SSO platform [44], that provides core identity services such as strong authentication and authorization mechanisms as well as support and implement a transparent single sign-on (SSO) procedure.

As indicated in the brief analysis of STORM main technological components, the proposed integration framework is totally based on open-source technologies and software tools, rendering the final product (STORM Environment) a cost-effective and easily adopted innovative solution. This critical characteristic could be also considered as the fundamental benefit and added value of STORM, given that nowadays, key organisational decision makers and business managers (e.g. CIOs, CISOs, CFOs, etc.) are seeking urgently and massively, in a constantly evolving pace, for more efficient and cost-effective risk management solutions in order to reduce operational costs and resist the existing economic crisis. Especially in cases where security is falsely considered as a secondary need and disregarded due to the required additional costs (outsourcing to security consulting companies to perform risk assessment and management activities), an efficient solution that is able to provide reliable risk assessment and management services at extremely low cost is considered as an indispensable property.

Achieving this, STORM constitutes an innovative security management platform that is able to confront and effectively manage the trade-off between low cost and security management expertise by harnessing corporate knowledge, leveraging existing infrastructures and boosting work productivity.

5 Conclutions - Future work

STORM is an open, innovative, collaborative security management environment, which can used in various organizations (from large organizations hosting critical

infrastructures to SMEs and mEs) in order to effectively address their security and privacy needs.

The STORM environment has been proposed [42] as the preferred solution in order to provide security management services to the port Information systems. It will also be implemented in the S-PORT project [49] funded by the National research program "Cooperation" (NSRF 2007-2013) of the GSRT (General Secretariat for Research and Technology Development Department) in three Greek commercial Ports (Piraeus Port Authority S.A., Thessaloniki Port Authority S.A, Municipal Port Fund Mykonos).

STORM has also been selected as the appropriate architecture for policy making in collaborative environments and it will be implemented in the E.C. FP7 project ImmigrationPolicy2.0 [30].

Acknowledgements. The authors would like to thank the GSRT for funding the S-Port project, and the E.C. for funding the ImmigrationPolicy2.0 project. Finally we thank the S-Port and ImmigrationPolicy2.0 partners for their contributions.

References

1. 3proxy: http://tools.securitytube.net/index.php?title=3proxy
2. Abele Wigert, I., Dunn, M.: An inventory of 20 national and 6 international critical infrastructure protection policies. In: Wenger, A., Mauer, V. (eds.) International CIIP Handbook 2006. vol. 1. ETH, Zurich (2006)
3. ADONIS: www.adonis-community.com
4. Agarwwal, A., Bellucci, D., Coronel, A., DiPaola, S., Fedon, G., Goodman, A., Heinrich, C., Horvath, K., Ingrosso, G., Liverani, R.S., Kuza, A., Luptak, P., Mavituna, F., Mella, M., Meucci, M., Morana, M., Parata, A., Su, C., Sureddy, H.S., Roxberry, M., Stock, A.: Owasp testing guide v3.0 (2008), http://www.maresystem.de/whitepaper
5. Autopsy: Autopsy forensic browser, http://www.sleuthkit.org/autopsy/index.php
6. Basel Committee on Banking Supervision: Sound practices for the management and supervision of operational risk. BSI, Basel, Switzerland (2001)
7. BCIGPG: A management guide to implementing global good practice in business continuity management. In: Good Practice Guidelines 2007. (BCI GPG) Business Continuity Institute (2007)
8. Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R.K., Raman, S., Chavan, U., Rathore, B.: Information systems security assessment framework (issaf) draft 0.2.1 (April 2006), http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1/view.html
9. BS25999-1: Business continuity management. British Standards Institute
10. Clinch, J.: Itil v3 and information security, ogc white paper (May 2009), http://www.best-managementpractice.com
11. COBIT4.1: It governance control framework. IT Governance Institute (2007), http://www.isaca.org

12. COBRA Methodology: Security risk analysis and assessment. http://www.riskworld.net/method.htm
13. CRAMM: Ccta risk analysis and management method, cramm version 5.2 information security toolkit (2003), http://www.cramm.com
14. ddrescue: http://freshmeat.net/projects/ddrescue/
15. Dnsmap: http://unknown.pentester.googlepages.com
16. DNSPredict: http://johnny.ihackstuff.com/downloads/task
17. Ebios: Expression des besoins et identification des objectifs de securite (2004), http://www.ssi.gouv.fr
18. ENISA: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools (2006)
19. ENISA: Cert exercises handbook. European Network and information Security Agency (2008), http://www.enisa.europa.eu/act/cert/support/exercise/files/handbook
20. EtterCap: http://ettercap.sourceforge.net/
21. ExploitDB: www.exploit-db.com
22. Fierce: http://ha.ckers.org/fierce/
23. Gooscan: http://johnny.ihackstuff.com/
24. HB292-2006: Handbook: A practitioners guide to business continuity management. Standards Australia, GPO Box 476, Sydney, NSW 2001, Australia (2006)
25. Herzog, P.: Osstmm:introduction and sample to the open source security testing methodology manual (osstmm 3 lite). Institute for Security and Open Methodologies (ISECOM) (August 2008), http://www.isecom.org/osstmm/
26. Honeynet: Honeynet project, http://www.honeynet.org/
27. Hping3: http://gd.tuwien.ac.at/www.hping.org/hping3.html
28. Httprint: http://net-square.com/httprint/
29. Hydra: http://www.thc.org
30. ImmigrationPolicy2.0: http://www.immigrationpolicy2.eu/
31. ISO/IEC:15408-1: Information technology - security techniques - evaluation criteria for it security – part 1: Introduction and general model (2005), http://www.iso.org
32. ISO/IEC:17799: Information technology - security techniques - code of practice for information security management (2005), http://www.iso.org
33. ISO/IEC:27001: Information technology - security techniques - information security management systems - requirements (2005), http://www.iso.org
34. ISO/IEC:27002: Information technology - security techniques - code of practice for information security management (2005), http://www.iso.org
35. John the Ripper: http://www.openwall.com/john/
36. Karantjias, A., Stamati, T., Martakos, D.: Advanced e-government enterprise strategies & solutions. In: International Journal of Electronic Governance (IJEG), Special Issue on Methodologies, Technologies and Tools Enabling e-Government. vol. 3, pp. 170–188. Inderscience Publishers (2010)
37. Medusa: http://www.darknet.org.uk/2006/05/
38. MEF: Metasploit exploitation framework, http://www.metasploit.com/
39. Metagoofil: http://www.edge-security.com/metagoofil.php
40. Nessus: http://www.nessus.org/nessus/
41. Nmap: http://www.insecure.org/nmap
42. Ntouskas, T., Polemi, N.: A secure, collaborative environment for the security management of port information systems. In: Proceedings of the Fifth International Conference on the Internet and Web Applications and Services, ICIW 2010. pp. 374–379. IEEE Computer Society Digital Library, Barcelona, Spain (2010)

43. OCTAVE: Octave method implementation guide version 2.0. Carnegie Mellon University (June 2001), www.cert.org/octave
44. OpenSSO8.0: https://opensso.dev.java.net/public/use/index.html
45. OpenVas: Open vulnerability assessment system, http://www.openvas.org/
46. Orrey, k., Lawson, L.J.: Penetration testing framework(ptf) v0.21. http://www.vulnerabilityassessment.co.uk
47. P0f: http://lcamtuf.coredump.cx/p0f.shtml
48. ProxyTunnel: http://proxytunnel.sourceforge.net/
49. S-PORT: S-port project, http://s-port.unipi.gr/
50. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical guide to information security testing and assessment. Special Publication 800-115, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
51. Sleuth Kit (TSK): http://www.sleuthkit.org/sleuthkit/
52. Stock, A.V.D., Lowery, D., Rook, D., Cruz, D., Keary, E., Williams, J., Chapman, J., Morana, M.M., Prego, P.: Owasp code review guide v1.1 (2008), https://www.owasp.org
53. Symfony: Symfony framework, http://www.symfony-project.org/
54. TCPtraceroute: http://michael.toren.net/code/tcptraceroute/
55. TinyProxy: http://tinyproxy.sourceforge.net/
56. ValIT: Enterprise value: Governance of it investments-the val it framework 2.0. IT Governance Institute (2008), http://www.itgi.org
57. Vallecillo, A.: Rm-odp: The iso reference model for open distributed processing,dintel edition on software engineering. pp. 69–99 (March 2001)
58. Volatility: Volatility framework, https://www.volatilesystems.com/
59. W3AF: Web application attack and audit framework, http://w3af.sourceforge.net/
60. Wack, J., Tracy, M., Souppaya, M.: NIST SP800-42:Guideline on Network Security Testing - Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-42, http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf
61. Wireshark: http://wireshark.org/
62. Zenmap4.60: http://nmap.org/zenmap/