ISO/IEC JTC 1/SC 22/OWGV N 0070

Report of the Application Security meeting, held in Glenburn Lodge (South Africa), Nov. 17th 2006

Date	30 April 2007
Contributed by	JTC 1/SC 27
Original file name	SC27n5482.pdf
Notes	Referenced by N 0071

ISO/IEC JTC 1/SC 27 **N5482**

REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Meeting Report (defined)

TITLE: **Report of the Application Security meeting, held in Glenburn Lodge (South Africa), Nov. 17th 2006**

SOURCE: Luc Poulin (co-rapporter)

DATE: 2006-12-07

PROJECT: WG 4 Study Period on Application Security

STATUS: This document presents outcome of the Application Security meeting held during the 1st SC27/WG4 meeting held in held in Glenburn Lodge (South Africa), Nov. 13th – 17th, 2006.

It is circulated within SC 27 for information.

ACTION ID: **FYI**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES 1 + 5

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.ni.din.de/SC27

Report of the Application Security

The Application Security group met during the 1st SC27/WG4 meeting held in Glenburn Lodge (South Africa) on November 13th – 17th 2006.

Participants

The following participants joint the meeting:

Name	Responsibilities
Kang Meng Chow	WG4 Convenor, SINGAPORE
Luc Poulin	Co-Rapporteur, CANADA HoD
Laura Kuiper	Co-Rapporter, USA HoD
Yasuo Miyakawa	JAPAN
Roslina Yusuf	MALAYSIA
Thay Yean Lan	SINGAPORE
Rosa Gracia Ontoso	SPAIN
Christine Simon	SWEDEN
Susanne Bjorkander	SWEDEN
Suhasini Sabnis	USA Expert

Agenda

The agenda as provided in ISO/IEC JTC 1 SC27 N5482 was accepted as follows.

1. Overview/Introduction
    a. Application Security (AS) Standard – Web Application Security (AS-W) Standards, proposed as a new work item in WG4.
2. Roll call of delegates
3. Confirmation of Agenda
4. Establish Study Period to
    a. Proposed objectives and scope of new standards
    b. Propose standards structure
5. Appoint Rapporteur for Study Period
    a. Luc Poulin, Canada & Laura Kuiper, USA
    b. US, Japan, Singapore to support the development
6. Request for NBs Contributions
    a. Contents
    b. Project Editors
7. Information Sharing
    a. RAISS Forum's draft Application Security Guidelines
        i. A section to do re-direction different users of the standard to relevant sections
        ii. Issue as a best practice guidelines in RAISS Forum
    b. Application Security, Canada presentation (N5488)
    c. Japan: Web application development guide and C/C++ coding guide being development in Japan, as part of NICT initiatives. Target for publication in April 2006, but will be in Japanese language. Will provide an update in next meeting.
8. A.O.B.
9. Closure of the meeting.

Meeting Application Security Objectives

On the first talk about Application Security, Mr Kang for Singapore presented the work from the RAISS Forum group, and the Canada was invited to make a speech about this subject. Mr Poulin presents a PowerPoint who resumes a part of his IT security class, from Laval University (see SC27N5488.)

The meeting concluded with the following decisions and follow-up actions (see WG4 Resolution SC27N5499):

1. Appointment of Mr Luc Poulin of Canada NB and Laura Kuiper of US NB as co-rapporteurs to initiate a six months study period in the area of Application Security.
2. The Project co-Rapporteurs to initiate a call for contributions from SC 27 NBs and liaison organizations.

The objectives and scope of the Application Security Project was also discussed and elaborated during the meeting. Appended below are the initial draft scope of contents to be covered in the project.

The next meeting of the application security will take place on 2007-05-04, Russia.

Application[1] Security (AS)

Objectives

The objectives this standard is to address emerging and existing security issues concerning the software application life cycle, including software development that are not covered by existing standardization work within the scope of ISO/IEC JTC 1/SC 27. The goal of this project is to develop a new group of standards documents to provide guidance and promote best practices to address common application security concerns. The standards are targeted for use by software application developers and understandable by managers and auditors.

Why Application Security is important

According to Gartner, at least 70% of the security breaches are from software leak and bugs. All security problems that can be solved with a software patch are an application security problem. If the development team, including the evolution team who develop new functionalities on an existing application, can integrate security requirements and best practices within the application life cycle, the cost on the security integration may be minimized and the risk on the security breaches may be reduced from the beginning of the application design and development. At the minimum, common security vulnerabilities resulting from insecure coding and development practices can be eliminated to provide a more secure and resilient codebase against common attacks.

Scope

- Integration of security concerns and requirements in the entire application life cycle
- Application security on it's all life cycle as the main focus
- Organization, developers and auditors are the mains targets audiences

Values/Benefits

- For the management:
    1. Help an organisation to create an secure application
    2. Minimize the impact, cost of security introduction on a system
    3. Help to identify the good level of trust for the contexts
    4. Know the control points and the security functions to be implemented and tested
    5. Receive a conformity proof on the level of trust targeted

- For the developers:
    1. To identify the control points and safety functions to be implement
    2. Minimize the impact of security introduction on their development process, tests and documentations.
    3. give many tools and bests practices to speedup the application development
    4. Increase the quality and the security of the application
    5. Make easier the Pairs review

- For the auditors:

[1] An *application* in this document is defined as a systemic point of view and include the software, the hardware, the data and the peoples implied in a system development and utilisation.

1. Provide all control points requested to prove the application reach the assurance level inside the targeted contexts.
2. Standardize the certification

Proposed Way Forward

A study period to develop a working document for the basis for a standardization project in the area of Application Security will last from November 2006 to the next WG 4 meeting in April 2007. WG 4 will consider the outcome of the Study Period for an NP in this area for recommendation to the SC27 Plenary in April 2007. Liaisons with all relevant ISO standards bodies, ITU-T Q9/SG17 and others standards organizations will be established.

ISO/IEC JTC1 SC27 WG4 will request the SC27 secretariat to issue a call for contributions.

Rapporteurs for this study period are:

- Luc Poulin
- Laura Kuiper

Topics for Inclusion

Examples of topics to be considered include:

- PART 1 – OVERVIEW, DEFINITIONS, CONCEPTS, AND PRINCIPLES
  - Introduction, Goal, Objectives, Scope
  - Terms and Definitions
  - Motivations
  - Targeted Audiences
  - Normative framework
  - Contexts Independencies
  - Security Issues/Risks Identification and Analysis
  - Assurance of trust (CC: Assurance Level)
  - Process level security concerns
  - Product level security concerns
  - Agile Development Methodologies
  - Environments
  - Application security process and verification control points
  - Development Processes and Techniques, including testing
  - Control and verification
- PART 2 – SECURE APPLICATION LIFECYCLE
  - Pre-requises and requirements
  - Generic Development Methodology
  - Agile Methodologies Mapping
- PART 3 – SECURE APPLICATION ARCHITECTURE DESIGN & DEVELOPMENT
  - Secure Application Architecture
  - Organizational identity management
  - Access control management
  - Security Design Patterns
  - Secure coding
- PART 4 – PROTOCOLS AND DATA STRUCTURE, INPUT, PROCESSES, AND OUTPUT SECURITY
  - Notation usage like UML, SAML, XACML, etc.
  - LDAP Directory
  - Other recommendations/guidelines from other bodies

- PART 5 – APPLICATION SECURITY ASSURANCE
  - Accreditation and Certification
- SPECIFIC Application Security type, as requested, like by example:
  - PART 6 – N-TIERS AND WEB APPLICATIONS SECURITY
  - PART 7 – CLIENT/SERVER APPLICATIONS
  - Etc …

Next step

- Develop new work item proposal (NP)
- Request for NB Contributions for contents and editorships
- Request for contributions and collaborative development with liaison organizations

Sources of Information

Identified sources of information as the first draft, but without limited at these sources:

- **ITU-T Q9/SG17**
  - SAML, XACML, …

- **SC7 – Software Engineering**
  - ISO/IEC 15504 CMMi® for Development (CMMI-DEV), Version 1.2 is an upgrade of CMMI-SE/SW/IPPD/SS, Version 1.1. The focus of the CMMI Version 1.2 effort is on improving the quality of CMMI products and the consistency of how they are applied.
  - ISO/IEC 20000 ITIL (Information Technology Infrastructure Library), the IT Service Management Standard
  - ISO/IEC 23026 Software Engineering. Recommended Practice for the Internet, Web Site Engineering, Web Site Management, and Web Site Life Cycle.
  - …

- **SC22 – Secure Coding**
  - …

- **SC27 – Security Architecture**
  - ISO/IEC 15408 Common Criteria
  - ISO/IEC 18028-2 Information technology -- Security techniques -- IT network security -- Part 2: Network security architecture
  - ISO/IEC 21827 Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®)
  - …

- **Information Systems Audit and Control Association (ISACA)**
  - CobiT (Control Objectives for Information and Related Technology)

- **Federal Information Processing Standards (FIPS)**
  - FIPS PUB 132 Guideline for Software Verification and Validation Plans (ANSI/IEEE 1012-1986)

- **Agile Software Development Methodology**

- Rational Unified Process (RUP)
- Enterprise Unified Process (EUP)
- …

- **American National Standard Institute (ANSI)**
  - ANSI INCITS 359-2004 RBAC, Role Base Access Control
  - …

- **National Institute of Standards and Technology (NIST)**
  - SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems,
  - SP 800-64 Series Security Considerations in the Information System Development Life Cycle
  - SP 800-80 Draft Special Publication 800-80, Guide for Developing Performance Metrics for Information Security
  - …

--- End of document ---