Chapter 1
Ontology-Based Analysis of Cryptography Standards and Possibilities of Their Harmonization

Alexey Y. Atiskov
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia

Fedor A. Novikov
St. Petersburg State Polytechnical University, Russia

Ludmila N. Fedorchenko
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia

Vladimir I. Vorobiev
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia

Nickolay A. Moldovyan
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia

ABSTRACT

Security means for shared computer, networking, and information resources are not balanced, inefficient, and poorly integrative. This chapter gives a brief overview of certain discrepancies and incompletenesses of ISO standards ISO 15408, ISO 18045, ISO 27k, etc., which are not balanced. Formal methods for their harmonization and coordination are described. Then the chapter discusses Hybrid Ontology Technology using Unified Modeling Language, State Transitions Model (state machine diagrams), and a special tool based on Equivalent Transformations of syntax graph-scheme.

DOI: 10.4018/978-1-4666-4030-6.ch001

INTRODUCTION

Nowadays security means for shared computer, networking, and information resources are not balanced, inefficient, and poorly integrative. It is primarily caused by the fact that the security object is a highly complicated nonlinear system having many degrees of freedom, but also by lack of balanced standards, regulations, structures, and policies.

In particular, the use of Russian (national) cryptographic standards such as:

- GOST 28147-89 "Information processing systems. Cryptographic protection. Algorithm of a cryptographic transformation,"
- GOST R 34.10-2001 "Information technology. Cryptographic protection of information. Processes of construction and verification for digital signatures,"
- GOST R 34.11-94 "Information technology. Cryptography information protection. Hash function" makes it impossible to certify cryptography systems according to the Common Criteria (ISO / IEC 15408:2005 Information technology—Security techniques—Evaluation criteria for IT security).

It is important to note that the set of regulating documents recently approved by ISO / IEC 15408 still plays an important role in unification and structuring of IT-security activities from organizational and technological points of view.

As compared with existing solutions, in particular, expert methods for cryptography standards analysis, ontology approach has certain advantages:

- Ontology provides an integral systematic view for the user as regards the group of cryptography standards;
- All the data on the standards are presented uniformly;
- All the synonyms are reduced to one notion, multi-valued (poly-semantic) words are referred to different notions, so there is no room for duplications or contradictions;
- Ontological model is an open one.

Important applications of the above approach include the analysis of security assurance analysis in cloud computing, i.e., the problems of user non-participation in control and protection of their information resources, which causes distrust in security and regulation of user data access, especially for legally relevant data. Cryptography means are preferable for security assurance in cloud computations. Moreover, user activities are not always transparent; therefore, additional complications arise in the sphere of compliance with standards.

That is why the essential problem as regards risk decrease is to provide proofs of effectiveness of cloud computing since security services in cloud technologies have been proposed but cannot be verified by the user.

BASIC PROBLEMS

Preliminary content analysis of standards based on semiformal models to be mentioned below revealed certain discrepancies and incompletenesses, in particular, concerned with ill-conditioned interpretations of the basic domain concepts such as Threat, Vulnerability, Asset, Countermeasure, Threat agent, etc., uncertainty of some primary concepts, and consequently incompleteness or inconsistency of certain provisions and recommendations.

These facts are most noticeable in the secondary national standard version, but the English-language original can hardly claim to be the logical perfection. Therefore, Committee JTC 1/