Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 13 (2018) pp. 149-158

Model Driven Approach for Designing of Information Security System

Ivan Gaidarski[1], Zlatogor Minchev[2] and Rumen Andreev[3]

[1]Joint Training Simulation and Analysis Center, Institute of ICT, Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl.25A, 1113 Sofia, Bulgaria
i.gaidarski@isdip.bas.bg

[2]Joint Training Simulation and Analysis Center, Institute of ICT, Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl.25A, 1113 Sofia, Bulgaria
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl.8, 1113 Sofia, Bulgaria
zlatogor@bas.bg

[3]Institute of ICT, Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl.2, 1113 Sofia, Bulgaria
rumen@isdip.bas.bg

***Abstract*: Reusability, interoperability, easy deployment and scalability are important requirements to the methodologies used for development of information security systems. A suitable way for solving this problem is the implementation of the conceptual modelling potential. In this paper is presented a model-driven approach to the development of an Information Security System. A conceptual model of Information Security System architecture is defined, using the main information security concepts, suggested from the framework of architectural description for the systems proposed by the standards IEEE 1471 and IEEE 42010. The rationality of this approach is mainly related to the developed conceptual models that contribute to the assigning of suitable architectural models of the information security systems of interest. The present approach is based on the assumption that the conceptual model is composed from meta-models of the various viewpoints. The result is a multi-layered concept system, presenting the relations between the concepts that describe the available viewpoints and relationships between them. Data centric models are accomplished, concerning different aspects of the data and data protection. The obtained results are based on the summary of the authors' practical experience in the information security activities. Further, the conceptual model is transformed into system design model with the help of UML – class, state, activity and deployment diagrams that transform the conceptual model of system architecture into an actual solution or physical system. Next, the presented idea is experimentally validated within interactive mixed environment simulation. Monitoring with access control of the exchanged data flows and used devices is also accomplished, using COTS DLP system implemented in the framework of the international cyber research exercise – CYREX 2018**

***Keywords*:** Conceptual Modeling, Data Protection, System Analysis, Architecture, UML

I. Introduction

Information is one of the most valuable asset possessed by the companies, as it provides a competitive advantage and is a prerequisite for their good performance on the market. Each asset must be considered in the context of its value and the associated risk of its loss. The field of security deals with the protection of assets, taking associated risk into account. The protection of information in all its forms is the main goal of Information security.

It is distinguished two methods for protection of the information assets with the vector of attack in mind. The first of them is Outside-In. It assumes that the attack to the assets comes from an external source - such as a hacker attack. The goal is to stop the attack from the outside and not to allow penetration to the resources of the organization. An example of such a solution is the firewalls. In the second method, the assets are protected in the direction Inside-Out. The presumption is that the attack is carried out by a person with access to the resources of the organization or an insider. The aim is to protect the assets so that it is impossible to be exported out even with a direct access to them. A typical solution is Data Loss Prevention (DLP). There are many commercial products that implement this method - for example Device Lock [3], Cososys Endpoint Protector [4].

Some of the security solutions realized in the information security systems are designed to be installed On-Premise - inside the organization. Typical On-Premise solutions are: Firewalls, Intrusion Detection System devices (IDS), Intrusion Prevention System (IPS) and Data Loss Prevention. Other solutions are designed for using to be used as services typically cloud based i.e. outside the organization. Typical service-oriented solutions are Threat Intelligence systems [5]. Of course, this division is conditional and depends on many factors - where information is stored, what are the policies of the organization in terms of its information, etc. Some of the traditional security solutions, which are typically implemented as On-Premise have options for cloud-based external services.

Information security (IS) activities applied within an organization concern compliance with certain legislative

regulations, necessary for its normal operation. There are IS standards such as ISO 27000 [6][7], ISACA's COBIT [8][9], NIST "800 series" [10], special sector-specific regulations - the Gramm-Leach-Bliley Act (GLBA) [11] for the financial sector, Sarbanes-Oxley Act (SOX) [12][13] for US public companies, Health Insurance Portability and Accountability Act (HIPAA) [14] and Payment Security Industry (PCI) Data Security Standard (DSS) [15] for credit card operators. While these standards and regulations incorporate the most important aspects of IS, they are rather a set of good practices. The cases, in which the IS are approached methodically and all requirements of the standards are satisfied, are seldom. Thus, the most common practice is single actions to solve certain tasks as incidents (leakage, attack on infrastructure, loss of information, etc.) or new challenges - for example recently adopted regulation EU GDPR [16] for protection and processing of personal data of EU Citizens.

The development of information security systems (ISS) can be done using two approaches – bottom-up and top-down. The former concerns the gradual protection of the information assets, starting with day-to-day activities through which system administrators try to improve the security of individual devices/applications. We apply a component-orientation approach to system analysis, which presents engineering-oriented architecting of information security systems (ISS). The main disadvantage of this analysis is that we find the constituent parts of an ISS as organizational units, process units, and information units and provides a single unifying view of the system. The engineering approach concentrates only on the DO ingredient of a domain analysis. It spreads over the deployment and technology aspects of a system development. The baseline models are determined by the available technologies, platforms and infrastructure and satisfy the needs of architectural representations that present deployable images of an ISS. The platform model describes the realization of the information infrastructure in terms of its implementation technology and its underlying communication infrastructure.

The shortcomings of the upper method can be avoided by the use of the top-down approach. It is based on goals set concerning management, predefined policies, procedures and processes, with specific results and clearly defined responsibilities and roles of the participants. This approach has a better chance of success because of the strong support of senior management, usually a budget, a pre-approved plan, and clear deadlines [1][2].

The main purpose of the ISS is to protect and secure the organization's information assets. An important requirement to contemporary methodologies for development of systems including ISS is to ensure the achievement of such system's properties as interoperability, reusability of their components, easy deployment and scalability. The engineering-oriented architecting of systems is not able to guarantee their achievement. Since the top-down approach to systems development is very suitable for this objective, we suggest the usage of model-driven architecting of Information Security Systems. On this basis, it is necessary to create a reference methodology for system development.

This approach is suitable for creation of a reference methodology for ISS development which bases on determination of a domain analysis framework that serves for construction of domain models. The main objectives of this framework coincide with the goals of the framework for architectural description of systems that is presented in the standards IEEE 1471 and IEEE 42010 [24][25]. They introduce concepts as View, Viewpoint, Stakeholders, Concerns and Environment which is related to the architecture description [26][27][28][29]. These concepts are workable in domain analysis and they guarantee a context for definition of a common conceptual framework, allowing the construction of conceptual models of ISS when the domain concerns information security [30], [31].

At present, there is much interest in using Unified Modeling Language (UML) for architectural description, since it provides tools for sketching, analyzing, modeling and documenting knowledge and solutions about the architecture of a software-intensive system as ISS. The UML support techniques that enable system developers to record what they are doing, modify or manipulate suggested architectures, to reuse parts of them that exist and to communicate the architectural information collected during system development. The goal of UML [28] is to provide a standard notation that can be used by all object-oriented methods. It provides constructs for a broad range of systems and activities (analysis, system design and deployment). UML consists of several diagram types providing different views of the system model.

The main objective of the paper is to present model-driven approach for designing of ISS that transform a conceptual model of system architecture into design model of the system, described with UML. In Section 2 we define a framework of domain analysis, in which we will construct our conceptual models. Section 2.1 defines the context of the conceptual modelling, while in the Section 3 and Section 4 we propose conceptual meta-models of ISS, based on the "Information Security" and "Information Processing" viewpoints, which is combined as Multi-Layered conceptual model in Section 5. Then the conceptual model is transformed to system design model with the help UML – class, activity, state and deployment diagrams. In the next Section 6, we show how with the help of the UML diagrams, real-world data protection tools can be deployed in the ISS.

In Section 7 we validate and the proposed models in a hybrid simulation environment that allows the combination of real and simulated activities into an interactive environment in the framework of the international cyber exercise – CYREX 2018 [38].

II. Framework for Domain Analysis

The definition of domain is symptomatic of persisting uncertainty. The systems that are developed in some domain do not necessary have to be highly similar. The domain model is an abstraction that consists of only those parts of domain knowledge that are relevant to a particular purpose. Domain models are an effective means for dealing with development of architectural description of a system – model-based architecting. We consider the usage of conceptual modelling as an approach to construction of domain models.

Domain analysis is the process of development of appropriate domain models. Here analysis refers to the examination of the domain, and appropriateness means that the domain model allows solutions to problems in a particular area of interest to be built up. A domain model should be a generic solution to a

class of problems from which to extract a specialization. The domain analysis is successful if it makes a distinction between knowledge that relates to subject domain, i.e. about problems to be solved and knowledge that relates to deployment domain, i.e. representations, methods and instruments helping the problems solution. This division of the domain is in correspondence with its definition - the domain is a field of knowledge and activities [A]

The main problem of domain analysis is to clear how a domain model is to be constructed, what representation is to be used and how the architecture description of a particular system could be derived from a domain model. This approach has several advantages in the guarantee of the main system's properties that are related to the possibilities to change a system:

- A domain model allows for more precisely expression of the requirements for a system that could be modified;
- The model may show that the building of a totally new system is more effective then to make changes in the existing system;
- Since the use of the domain model is not limited to a single application, the cost of its construction can be spread out.

The construction of a framework of domain analysis is conformed to the following principles:

- Framework objectives. To allow the analyzers of different communities to use a common terminology in domain modelling in order to avoid details.
- Determination of domain ingredients. An area of interest could be analyzed on the base of the following questions – Why, What, How to Operate and How to Do (Deployment and Technology). A complete answer to each question requires several viewpoints (VP) to the domain. Par example, the clarifying of "How to Do" ingredient requires the following viewpoints in a computer-oriented domain - information viewpoint (focuses on information processing and relationships between information objects), computational viewpoint (focuses on functional specification and decomposition, system design), engineering viewpoint (focuses on how to solve distribution issues), and technology viewpoint (focuses on specific technology and solutions).
- Principles of Viewpoints definitions. Each viewpoint is an abstraction that helps to illuminate a specific domain aspect. The different viewpoints belonging to different stakeholders.
- Principles of conformance, consistency, specialization and realization. Viewpoints provide a set of viewpoint consistency rules based on correspondences between the core modelling concepts of the different viewpoints. One is therefore able to correlate different formulations of the same or related abstract concepts in different views of the system.
- The area of interest covered by a domain is presented by concerns. A Concern expresses a specific interest in some topic pertaining to a particular system of interests. Each viewpoint addresses concerns that are system development issues. Stakeholders have Concerns. Concerns (and stakeholders) arise at all stages of the system life cycle from conception, through requirements, design, implementation, maintenance and evolution. The relation of concerns to stakeholders is many-to-many.
- Principles of scientific concept formation. Since the domain models have to relate to an understanding of all activities concerning system development, we need a model for the formation and comprehension of the concepts that arise in the domain. It is necessary to construct a concept model that assists in the interpretation of the structure of the domain. That is why the construction of domain models concerns conceptual modelling extracts from a universe of Activity (UoA) that is called concept space or concept domain. The conceptual modelling has the following purposes:
- To determine the base concepts of particular area of interest and to define the concept space, which is a system of concepts;
- To determine a way of linking between the basic concepts of different concept spaces of different domain ingredients.

The Viewpoint captures the conventions for constructing, interpreting and modelling a type of view that is in relation to a specific Model Kind, which provides specific forms of representation, with its own meta-model (What) to address one or more identified concerns (Why), via associated methods and practices (How) [19]. Viewpoint modelling is a kind of meta-modelling (Concepts formation), whose result is a way to make models (views) of a certain kind [20].

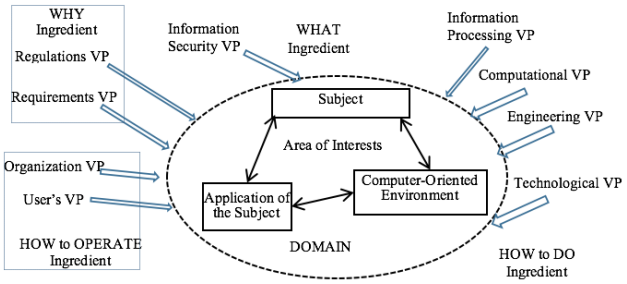


Figure 1. A framework for domain analysis.

A View is a representation of a domain aspect from the perspective of a related set of concerns. Each view corresponds to exactly one viewpoint. It is addressed to stakeholders of a system that is developed to solve some problems concerning the domain. A view has a model orientation, which declared the purpose, context, and a governing viewpoint and is comprised of architecture models of the system that realizes.

The framework for domain analysis as a system of viewpoints helps to achieve a domain-driven conceptual modelling integration, since the domain model determines the baseline model of stakeholders' roles and portions of the architecture model of a system.

The Context of Conceptual Modelling

According to the ancient Greeks concept formation is arisen in a framework of thoughts that constitutes of four components: idea, image, material (objects) and concepts (Figure 2) [17]. Concepts are in relationship with objects and their represented images, which are in our focus and determine a concepts

domain. The Russian scientist Vygotsky concentrates on the psychological aspects of the concepts development. He designates two groups of concepts that concern different levels of their formation – spontaneous concepts and scientific concepts. They are considered in Chapter 6 of [18]. His research on the development of scientific concepts (i.e. true concepts) clarifies the most basic and essential general laws of concept formation.

The spontaneous concept is characterized by a lack of conscious awareness. Attention is always directed toward the object that the spontaneous concept represents rather than on the act of thought that grasps that object. The concept becomes something different as soon as it is considered in a system of concepts. The nature of spontaneous concept changes as soon as it is pulled out from its isolated form, in which it provides a simpler and more immediate relationship to the object and placed in a system of concepts. The presence of a concept system is significant for the nature and structure of each individual concept. If a higher concept arises on a given concept, there must be several subordinate concepts that include it. The relationships of these other subordinate concepts to the given concept must be defined by a system created by the higher concept. In this way, the generalization of the concept leads to its localization within a definite system of relationships of generality that are the most natural and important connections among concepts. Thus, at one and the same time, generalization implies the conscious awareness and the systematization of concepts.

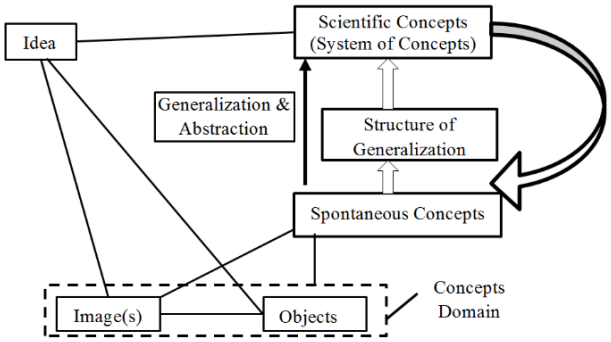


Figure 2. Framework of concept formation.

Conscious awareness and the presence of a system are synonyms when it is considered concepts, just as spontaneity, lack of conscious awareness, and the absence of a system are three different words for designating the nature of initial concept development. If conscious awareness means generalization, it is obvious that generalization, in turn, means nothing other than the formation of a higher concept in a system of generalization that includes the given concept as a particular case. Each structure of generalization has a characteristic degree of unity, a characteristic degree of abstractness or concreteness. For each stage of generalization, there is a corresponding system of relationships and generality. General and specific concepts are ordered in a genetic series in correspondence with this system. Thus, in concept development, the movement from the general to the specific or from the specific to the general is different for each stage in the development of meaning depending on the structure of generalization dominant at that stage.

The scientific concept necessarily presupposes a different relationship to the object, one which is possible only for a concept. It is not related to its object directly. This relationship is mediated through existing concepts that themselves have an internal hierarchical system of interrelationships. The dependence of scientific concepts on spontaneous concepts and their influence on them stems from the unique relationship that exists between the scientific concept and its object. Consequently, in its relationship to the object, the scientific concept includes a relationship to another concept, that is, it includes the most basic element of a concept system. This existing system is a prerequisite for the development of the new system. In the development of scientific concepts, the system emerges only with the development of the scientific concept.

III. Conceptual model of information security viewpoint

The meta-model of the viewpoint “Information Security is important for stakeholders like developers and integrators. Their concerns include conceptual integrity, deployment, scalability, reusability, structure, system properties. From the “Information Security” viewpoint, ISS has to answer to some questions: What must be protected, Why it has to be protected and How it can be protected? To answer these questions, we propose a meta model, which consists of 7 concepts (Figure 3): endpoint protection, communications and connectivity protection (what); security monitoring, security analysis, and security management (how); data protection and security model and policy (why). Each of these concepts is related to specific component with a specific role and characteristics.

Endpoint Protection delivers protection capabilities for the endpoints. It provides functionalities as identity management, cyber security tools and physical security. The Communications and Connectivity Protection is responsible for protecting the communication between the endpoints. It implements different methods as authentication, authorization, cryptographic techniques and information flow control. Securing the endpoints and communications is important, but the state of the system cannot be maintained without constant monitoring, analyzing and controlling all components of the system. That is the main role of the next three components – Security Monitoring, Security Analysis and Security Management.

The implementation of security policies is the main function of the Security Policy component. Its main goal is to ensure confidentiality, integrity and availability of the system. It instructs the other components how to work together to ensure the security of the system. The objective of the last component, Data Protection, is to protect all data in the system. It supports the rest of the components, as they all dealing with some data - data-at-rest in the endpoints, data-in-motion in the communications, data gathered as part of monitoring and analysis modules and all data from the system management [21].

To achieve the goals of information security, each component (concept) is realized through appropriate instruments – Information Security Techniques (IST), which include security tools and procedures that addresses and reduces the threats to the system and helps ISS components to perform their basic functions. Three basic categories of IST could be defined: Physical, Technical and Administrative:

- Physical: Restricts direct physical access to equipment and keep the integrity of the system. Applies to all components of

ISS and include: System and Data backups, Backup power supplies, Keys, Keypads, Locks, Cipher locks, Biometric access controls, Keyboard locks, Fences, Security guards, motion, smoke and fire sensors, CCTV monitoring and alarms.

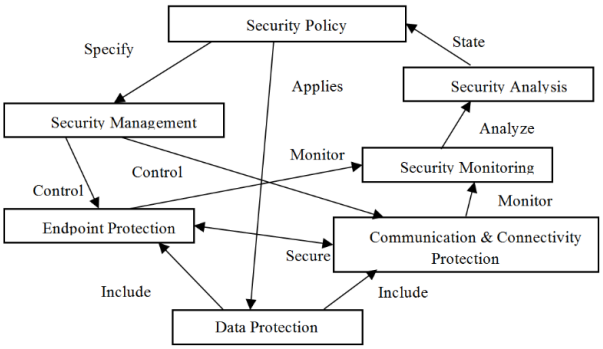


Figure 3. Meta model of information security viewpoint.

- Technical: Part of the Endpoint Protection and the Communications and connectivity protection components. They can be hardware and software and usually work autonomously without human intervention: Firewalls, Access control systems, Digital signatures, Smart cards, Passwords, Network management tools; Antivirus software, Audit trails, IDS and IPS (Intrusion detection and prevention), DLP (Data Leak Prevention) and etc.
- Administrative: Applies to the Security Model and Policy component and determines the rights of the users dealing with organizational resources. Among these IST are Information Security policies and procedures, Management and supervision, Data/resource ownership, Authorization for access to resources, Security reviews and audits Security awareness and training, Disaster recovery and contingency plans, Separation and rotation of duties and Performance evaluation [22].

Endpoint Protection

Endpoints are elements of ISS that have computational and communications capabilities: devices, workstations, servers, communications infrastructure elements and etc. They have different functions and security requirements and their protection can be achieved with specific IST.

To ensure the availability, confidentiality and integrity of the endpoint, the component must guarantee the existence of the following security characteristics (Figure 4):

- Endpoint Physical Security: It ensures physical protection of the endpoint to prevent unauthorized changes and is realized through ISTs as theft prevention and anti-tampering mechanisms;
- Endpoint Root of Trust is a result of the rest of the functions at the endpoint - it supports both the hardware and software including firmware, operating system, execution environment and application;
- Endpoint Identity bases on mechanisms for identification of the endpoint;
- Endpoint Integrity Protection is consequence of the integrity of the endpoint;
- Endpoint Access Control bases on the authentication and authorization before giving access to the services and resources;
- Endpoint Configuration & Management presents the control of the security policy and manages the configuration of endpoint - it includes security updates and patches;
- Endpoint Monitoring and Analysis guarantees monitoring of the other characteristics: It performs detection, prevention and recovery from any deviation from the security policy of endpoint together with Endpoint Configuration & Management. It also ensures detection of the malicious patterns, DoS activities, security policies enforcement and security performance indicators tracking;
- Endpoint Data Protection ensures the confidentiality, integrity and availability of endpoint's data, including operational, monitoring and configuration data: It uses IST like access control, encryption and isolation;
- Endpoint Security Policy is necessary for the management of the execution of the security policy in the endpoint.

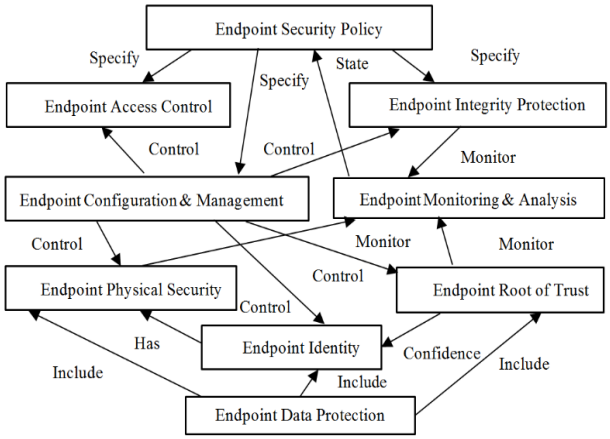


Figure 4. Endpoint protection idea.

Communications and Connectivity Protection

The characteristic ensures the physical security of connected endpoints and communication channels, cryptographic protection of communications, and information flow protection. Communication and Connectivity Protection integrates the following security characteristics (Fig. 5):

- Physical Security of Connections provides protection of physical connectivity layer.
- Communicating Endpoints Protection secures the communication between endpoints.
- Cryptographic Protection ensures authenticity of communicating sides and the integrity and confidentiality of the data, by using cryptographic technologies.
- Information Flow Protection provides that only permitted content pass the communication channel. It uses IST like network isolation, segmentation and perimeter protection.
- Network Configuration and Management provides enforcement and control of security policy and manages the configuration of other components. It includes configuration of gateways and firewalls,

segmentation of the network and cryptographic protection.

- Network Monitoring and Analysis performs monitoring and analysis of the network data. It includes IST like access control, deep packet inspection, intrusion detection and log analysis.
- Data Protection ensures the confidentiality, integrity and availability of the communicating data.
- Security Policies for Communications and Connectivity Protection directs the execution of security policies and defines how the network components communicate with each other.

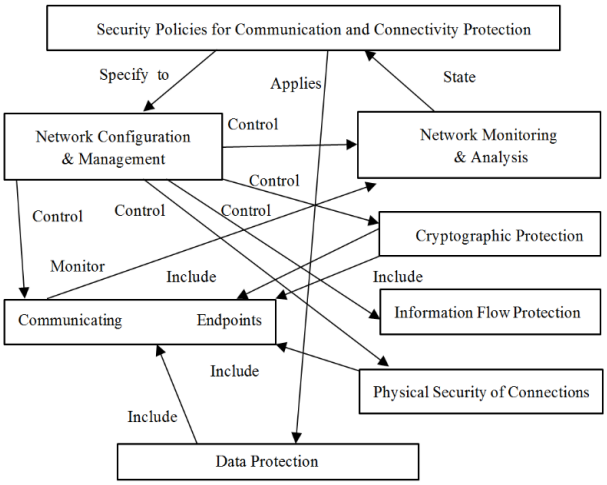


Figure 5. Communications & Connectivity Protection.

Multi-Layered Conceptual model of Information Security System

For the construction of a conceptual model of ISS it is necessary to present the meta-models of all viewpoints. We are limiting to the description of the conceptual model of the viewpoint "Information processing" that is the second layer of the constructed multi-layered model of ISS (Fig.6). It focuses on the different states of the data and their processing and covers all possible data in the system - the processed (operational) data, the configuration and monitoring data. In general, the data can be in one of the following states: Data-at-Rest, Data-in-Use or Data-in-Motion [1]:

- Data-at-Rest – Inactive data, stored in databases, data warehouses, archives, tapes, spreadsheets, backups, workstations, laptops, file servers;
- Data-in-Use – Active data under constant change, processed or used in applications, printed on local printers, stored on USB devices, CD-ROMS;
- Data-in-Motion – Data transmitted across connections between endpoints, transmitted across the network, temporarily residing in computer memory to be read, printed on network printers, being copied from one location to another.

Figure 7 shows the two layers, which contains the meta-models representing "Information security" (Layer1) and "Information processing" (Layer2) viewpoints respectively and the relations between their components. The resulting multi-layered model will give additional properties of their components and will combine their functionality with new features, giving answer to the question "How information can be protected".

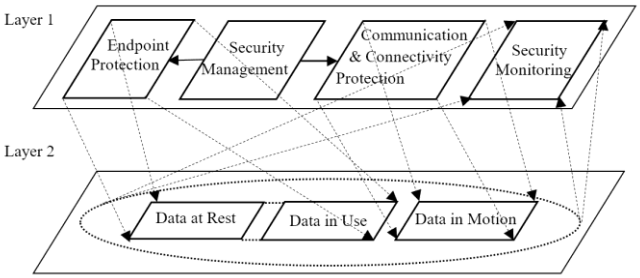


Figure 6. Meta-model of "information processing" viewpoint of ISS.

For protecting the data different strategies can be executed, depending from the type of data. The different kinds of threat to the data (loss, theft, unauthorized access or uncontrolled changes) also define how they must be protected. The level of protection depends from the accepted risks and costs. To answer the question, specific IST can be applied on the components of meta-models [1][2][32]:

- The Endpoint Protection characteristic must protect all the data on the endpoints, including configuration, monitoring, and operational data, so it is linked with Data-at-Rest and Data-in-Use. The relevant IST are access control and passwords, antivirus, data leak prevention (DLP) tools, audit trails, physical security measures and etc.;
- Communications and Connectivity Protection addresses Data-in-Motion - to secure communications and protect authenticity, integrity and confidentiality of exchanged data. The relevant IST includes cryptographic technologies, network segmentation, perimeter protection, gateways, firewalls, intrusion detection, network access control, deep packet inspection and network log analysis;

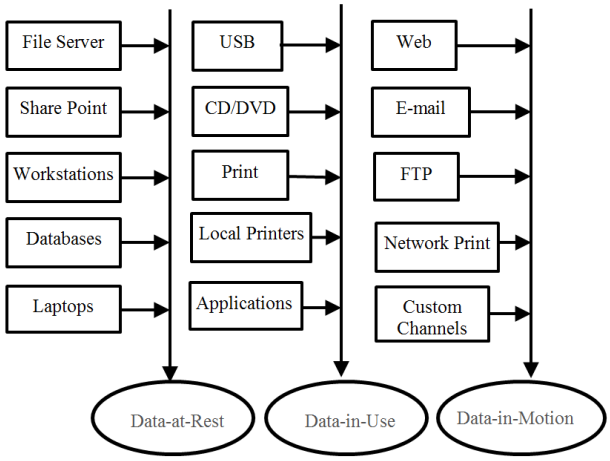


Figure 7. Two-Layered Conceptual Model of ISS.

- Configuration and Management Protection is responsible for all data related to configuration of Endpoint Protection and Communications and Connectivity Protection using relevant IST as cryptography;
- Monitoring and Analysis Protection is tracking the current state of the system, perform monitoring of the activities, key system parameters and indicators, insuring the system trustiness - The typical IST are cryptographic techniques.

IV. UML Design Model

System development lifecycle consists from the following processes:

- Requirements gathering processes – resulting in requirements model.
- Analysis processes to understand the requirements – resulting in an analysis model, describing implementation-independent solution which satisfies the requirements model.
- Design processes – resulting in design model, which describes implementation-specific solution, specified by the analysis model.
- Implementation processes to build a system – resulting in implementation model of physical system that satisfies the design model.
- Testing processes – to verify that a system satisfies its requirements.
- Deployment processes, to make the system available to the users.

Each process results in the corresponding model, which satisfy the previous requirements and is a base for the next level model [35][36]. The whole process of system development is a model-to-model transformation. One of the most convenient ways is to use object-oriented tool as UML. In our approach, we show the transformation from conceptual model into UML design model [32]. For the description of the proposed Multi-layered meta model of ISS it is necessary to describe the system concepts, the different activities and system implementation. It can be done, using different UML diagrams: for description of the system concepts - UML Class Diagram, for description of the dynamic aspects of the system – UML Activity Diagram and for the implementation of the ISS's components – the UML Deployment Diagram [32][36].

To represent the different states of the data in the system, the UML State diagram is used – Fig.8.

We use different agents, which are responsible for the respectively data processing and transformation. The Endpoint Protection Agent is responsible for the protection of the data in the endpoints, the communication Protection Agent is responsible for the network and communication data protection and the Services agent is protecting the data from the system's (organization) services.

All of these data channels are monitored by the Monitoring Agent, and compared with the accepted Data Policy by the Policy Agent. The data policy includes rules and dictionaries with keywords, which defines the sensitive data, which must be protected in the ISS. If the data is recognized as sensitive by the Policy Agent, then a data breach is occurred. In this case the Breaching Agent, which is responsible for handling the data breaches, act according the rules in the accepted Data Policy. The Breaching Agent sends a breach report to the Reporting Agent, which generates log for the breach, including different parameters as user, time, place, operations, data channel, application, protocol and etc. If Data Policy involves backing up the leaked data for investigation or other purposes, the Storing Agent is activated to perform the corresponding action.

The Storing Agent stores the data securely, along with all relevant data – time, users, operations, IP addresses, place of the data breach and etc. If the Data Policy determines a stop of the leaked data on relevant channel, the data is stopped otherwise it is processed by the Processing Agent. It is already reported and potentially stored for investigation.

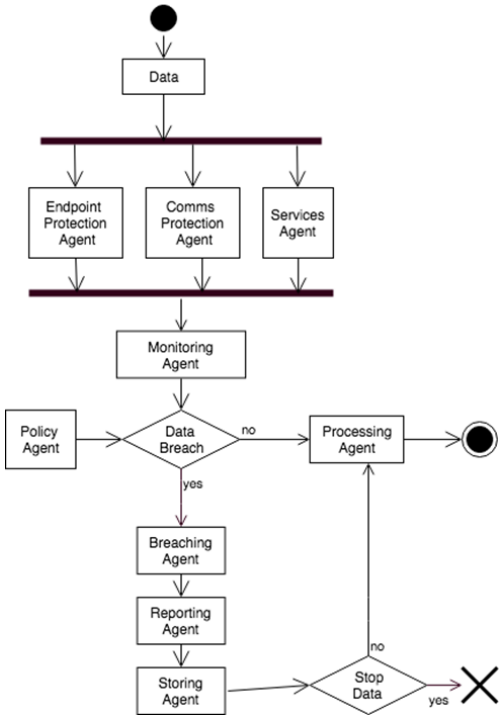


Figure 8. UML State Diagram.

Alternatively, if the Policy Agent does not recognise data breach, the data is processed by the Processing Agent.

Data Protection Tools and Their Deployment as Part of the ISS

The traditional network- and infrastructure- centric security solutions for protection of the data (gateways, firewalls, network segmentation, intrusion detection and others) are designed for protection, monitoring and control of threats with outside-inside vectors of attack. They are not enough when it comes to protection of sensitive information. A new kind of tools is needed, which are capable on protecting the data from inside-outside direction [33].

Such solutions, which leverage data-centric approach, are the Data Leak Protection (DLP) systems [3][4]. They are designed to stop data leakages from inside to the outside, no matter it is intentional or unintentional, being a result of a human errors. DLP systems are capable on preventing the attempts to steal, modify, prohibit, destroy or obtain unauthorized access to the data, by detecting its content and enforce protective actions based on the value and level of importance. DLP systems combines contextual and content analysis methods, enforcing centrally managed data protection policies. In order to protect the data in all possible states, DLP solutions recognize and control the three data types: Data-In-Use, Data-In-Motion and Data-at-Rest - Fig.9 [34].

DLP systems are able to protect the data, according to the behaviour of users. They are easy tools for achieving compatibility with different security regulations, standards, internal rules and security policies. DLP systems can control all global communications and data channels of the organization – Fig.10[3].

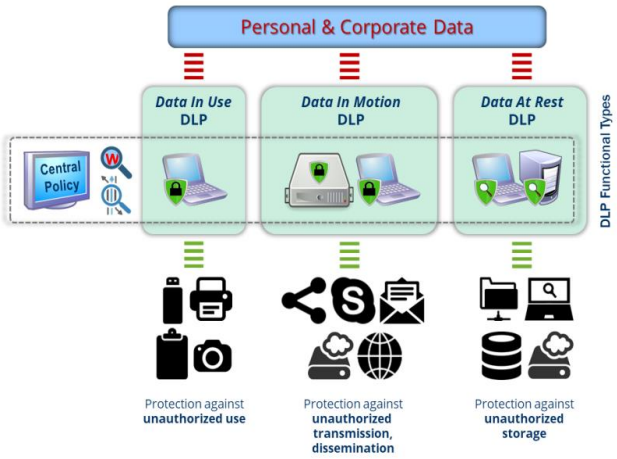


Figure 9. Data Leak Prevention (DLP) solution.

Figure 10. DeviceLock DLP suite.

V. Practical validation

The validation of the accomplished analytical modelling findings was further conducted empirically, implementing a transformed reality interactive simulation, organized in the framework of CYREX 2018 [37].

Using a fictitious scenario events script, played (for about 180 minutes) from the trainees in several multirole teams, an exploration of digital transformation plausible future data relativities dynamics was performed.

The scenario architecture included four key attack vectors (social engineering, industrial espionage, malware & targeted attacks) and seven main teams, organized as follows: a start-up company – 'Digital Creativity', developing a payment solution, based on human capabilities digital copying. The innovative results are bought from a larger corporation – 'Moon Digital Solutions', which has some invading plans on the 'New Life' planet colony.

A hacker group 'Stellar Ghost' is also involved, modifying the 'Digital Creativity' work, swapping the data with aggressive dictatorship and fighting skills for the robots at 'New Life'. Other exercise participants were: 'Galactic World' – an intergalactic association responsible for digital techs regulation, using another small company – 'QHR Selection' to interfere in the situation and stop the hackers' terrorist plans, giving the 'New Life' colony robots fast food skills instead of aggressive ones. Finally, a PR body – 'Stellar Media' is involved for assuring public announcements of the situational dynamics.

Figure 11. Moments and architecture of CYREX 2018, exploring data relativities digital transcending [37].

The participants used several device types: phablets, tablets, desktop and mobile computers, numerous open cloud services (data storage and sharing, encryption, chats, social media, multimedia messaging, e-mail accounting and participants DLP multi asset configurable monitoring) some accessed directly or with encrypted QR codes. The exercise was mainly organized in a closed Facebook social network group, partially implementing also WhatsApp & Viber, while participants' network access to the used cloud services was organized via a VPN. The players' behaviour was explored and archived remotely, using response time monitoring, video recording (similar to CYREX 2017 [38]) and COTS DLP solution CoSoSys My Endpoint Protector, v. 4.7.4.7 [4]. The DLP environment is capable to control 'Data-in-Motion' and 'Data-in-Rest' types of data. Based on client-server architecture the environment is providing client agents, installed on the users' endpoint devices, archived in a remote server. These agents are practically capable to control all the communication channels used in the exercise. The accomplished DLP solution is able to detect the content of the data and to compare it with preliminary defined keyword dictionaries, distinguishing sensitive data, whilst coping multiple I/O interface devices and allowing ad-hoc security policy definitions. The implemented users' monitoring approach provided an opportunity for deeper trainees' analysis, concerning their cognitive and behavioral responses.

Results Assessment

Having empirical nature, the accomplished framework of CYREX 2018 was quantitatively assessed (see Figure 12) from the participants (using trained teams inputs of both 'Positive' and 'Indefinite' indicators' percentage measures and the ideas marked in [39]), regarding five key parameters: 'Environment Adequacy', 'Scenario Complexity', 'Technological Effects', 'Human Factor Effects' & 'Training Satisfaction'. Additionally, DLP monitoring data log leakages aggregated and normalized results distribution is also given, regarding seven of the exercise monitored attacks: 'Unauthorized Devices Connection', 'Targeted Attacks', 'Marked Key Words', 'Malware', 'Delayed Responses', 'Social Engineering' and 'Equipment Fails'. The obtained validation results are addressing obvious successful understanding for CYREX 2018, compared to CYREX 2017 [38], giving only a diminished mark for the 'Human Factor Effects' asset (<< 70%) due to the hidden participants

monitoring that was not preliminary announced. Similar is the situation with the data leaks results, using insiders for installing specific key words in the teams communication language, together with provoking unexpected equipment fails and DDoS targeted attacks that were however indirectly successful (<< 10%), providing (>> 20%) visible delays towards the scenario scripts and unauthorized equipment (USB sticks and other peripheral devices with storage functionality) usage. Being more visible the malware and social engineering attempts in CYREX 2018 were getting better visibility (>> 15%), providing successful coverage for the unnoticed data leaks.

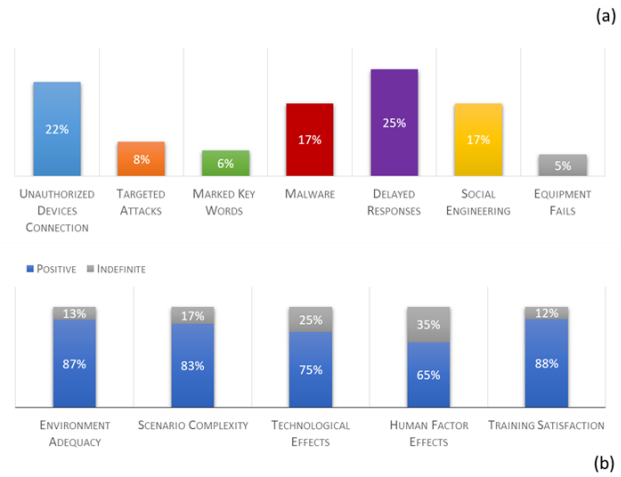


Figure 12. CYREX 2018 data leakage assets (a) and event aggregated assessment (b) results.

VI. Conclusions

The use of Conceptual Modelling as a tool for architecture description of ISS is important, since architecting involves getting to the fundamentals, deeper understanding, often reformulating the problem, while working on possible solutions.

The conceptual modelling improves the understanding among the participants in the development of systems of interest. The shared understanding is also the basis for reuse and interoperability. The introduction of first-class generalizations of the concepts of interest into conceptual models guarantees formalization that makes possible affirmation of an open implementation approach for improving our tools. In fact, abstraction is the core of conceptual modelling. However, the challenge is to connect high-level abstractions to lower-level abstractions, such that the systems architecture offers concrete guidance to designers and engineers.

In order to meet the objectives of information security policies in enterprises, a combined work of real-time systems (firewalls, DLP – Data Loss Protection systems, IDS – Intrusion Detection Systems, E-mail protection systems, Cyber Security tools) is required, as well as the efforts of various IT professionals. Typically, this is done according to the requirements of different security standards, know-how from practice and ad-hoc additional tailoring. The proposed approach enables the information security in the enterprises to be placed on a stable basis – through system of concepts, models and viewpoints, we make it possible to define the requirements and to implement them with real systems with the help of templates, specific for different industries and organizations, while maintaining interoperability and ensuring repeatability.

Acknowledgements

The research is supported by the KoMEIN Project (Conceptual Modeling and Simulation of Internet of Things Ecosystems) funded by the Bulgarian National Science Foundation, Competition for financial support of fundamental research (2016) under the thematic priority: Mathematical Sciences and Informatics, contract № DN02/1/13.12.2016. Additional gratitude is also given to the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES) 2018-2020", financed by the Ministry of Education and Science.

References

[1] Rhodes-Ousley M. *Information Security the Complete Reference, 2nd Edition*, pp. 303, 234-238.The McGraw-Hill (2013).

[2] Whitman,M., Mattord,H. *Principles of Information Security, Fifth Edition*. Course Technology, Cengage Learning, 2016

[3] DeviceLock www.devicelock.com/products/, last accessed 2019/04/08.

[4] CoSoSys Endpoint Protector www.endpointprotector.com, last accessed 2019/04/09.

[5] Arctic Security https://arcticsecurity.com, last accessed 2019/04/08.

[6] Hintzbergen, J., Hintzbergen K. *Foundations of Information Security Based on ISO27001 and ISO27002*. pp. 149, Van Haren (2010).

[7] ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html, last accessed 2019/04/08.

[8] IT Governance Institute. *COBIT Security Baseline: An Information Survival Kit. 2nd ed*. pp. 14. IT Governance Institute (2007).

[9] COBIT resources: http://www.isaca.org/COBIT/Pages/default.aspx , last accessed 2019/04/09.

[10] NIST Special Publications (800Series): https://www.nist.gov/itl/nist-special-publication-800-series-general-information, last accessed 2019/04/09.

[11] Gramm-Leach-Bliley Act (GLBA) Resources: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, last accessed 2019/04/09.

[12] Anand, S.: Sarbanes-Oxley *Guide for Finance and Information Technology Professionals*. pp. 93. John Wiley & Sons (2006).

[13] Sarbanes-Oxley Act SOX Resources: https://www.sec.gov/spotlight/sarbanes-oxley.htm, last accessed 2019/04/08.

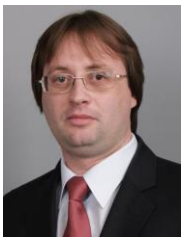
[14] Beaver, K., Herold R. *The Practical Guide to HIPAA Privacy and Security Compliance. 2nd ed*., pp. 4. Auerbach (2011).

[15] PCI Security Standards: https://www.pcisecuritystandards.org/pci_security/, last accessed 2019/04/08.

[16] EU General Data Protection Regulation Official Page: http://ec.europa.eu/justice/data-protection/reform/index_en.htm, last accessed 2019/04/08.
[17] Solvberg, A. Data and What They Refer to. P.P. Chen et al. (eds), *Conceptual Modeling, LNCS*, pp. 211-226, 1999, Springer-Verlag, Berlin.
[18] Vigotsky, L. *Thought and Language*, MIT Press, USA, 1962
[19] Hilliard R. *Aspects, Concerns, Subjects, Views, First Workshop on Multi- Dimensional Separation of Concerns in Object-Oriented Systems (OOPSLA'99),* pp. 1-3 (1999).
[20] Hilliard, R. *Viewpoint Modeling. In: First ICSE Workshop on Describing Software Architecture with UML*. Position paper. May 2001.
[21] Industrial Internet of Things Volume G4: Security Framework: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf, May 2017, pp. 46-61, last accessed 2019/04/08.
[22] Killmeyer J. *Information Security Architecture: An Integrated Approach to Security in the Organization*, pp. 203-240. CRC Press, Taylor & Francis Group, LLC (2006).
[23] Hornby, D.S., Cowie, A.P. and Gimson, A.C. *Oxford Advanced Learner's Dictionary of Current English*. Oxford University Press, 1974.
[24] IEEE Std 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems (2000).
[25] ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description: https://www.iso.org/standard/50508.html, last accessed 2019/04/08.
[26] IEEE Std 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems (2000).
[27] ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description: https://www.iso.org/standard/50508.html, last accessed 2019/04/08.
[28] OMG. Unified Modeling Language (UML), v. 2.5.1 https://www.omg.org/spec/UML/2.5.1/ last accessed 2019/04/08.
[29] Hilliard R. Using the UML for Architectural Description, Integrated Systems and Internet Solutions, Inc., Concord, MA USA, *in Proceedings of UML'99, Lecture Notes in Computer Science, volume 1723*, pp. 1-15. Springer (1999).
[30] Fernandez E. *Security Patterns in Practice*, pp. 25-50, John Wiley & Sons (2013).
[31] Breu R., Grosu R., Huber F., Rumpe B., Schwerin W. *Systems, Views and Models of UML. In: The Unified Modeling Language, Technical Aspects and Applications*. Martin Schader, Axel Korthaus (eds.) pp. 3-8. Physica Verlag, Heidelberg (1998).
[32] Gaydarski, I., Minchev, Z., Andreev, R. Model Driven Architectural Design of Information Security System, *14th International Conference on Information Assurance and Security (IAS 2018),* 13-15.12.2018, Porto, Portugal, Advances in Intelligence Systems and Computing, Springer, in press
[33] Gaydarski, I., Minchev, Z. Virtual Enterprise Data Protection- Framework Implementation with Practical Validation, *Proceedings of BISEC 2018*, Belgrade Metropolitan University, 20.10.2018, Belgrade, Serbia, DOI:10.13140/RG.2.2.19996.33925
[34] Gaydarski, I. Challenges to Data Protection in Corporate Environment, Chapter 8, In Z. Minchev, (Ed) *Future Digital Society Resilience in the Informational Age*, Institute of ICT, Bulgarian Academy of Sciences, in press
[35] Alhir S. Understanding the Model Driven Architecture (MDA), *Methods & Tools, 11(3),* 17-24 (2003).
[36] Dennis A., Wixom B., Tegarden D. *System Analysis & Design – An object-oriented approach with UML - 5th Edition*, pp. 19-52. John Wiley & Sons (2015).
[37] Cyber Research Exercise - CYREX 2018 Web Page, http://securedfuture21.org/cyrex_2018/cyrex_2018.html
[38] Z. Minchev, L. Boyanov, A. Georgiev, & A. Tsvetanov, "An Analytical Outlook towards Digital Training Security Transformations", *In Proc. of ICAICTSEE – 2017*, UNWE, Sofia, Nov 3-4, 2017, https://dx.doi.org/10.13140/RG.2.2.20333.28645

Author Biographies

Ivan Gaidarski (b. 1972, Hissar, Bulgaria) is a research assistant at Joint Training Simulation and Analysis Center, IT for Security Department, Institute of ICT, Bulgarian Academy of Sciences (2019); Educational background: Engineer on Computer Systems, Technical University - Sofia, (1998); PhD Student, Information Security, Institute of ICT, Bulgarian Academy of Sciences (2017 – 2019); Cyber Security expert at Joint Training Simulation and Analysis Center, IT for Security Department, Institute of ICT, Bulgarian Academy of Sciences, (2018); Main research areas: development of information security systems, Design & application of DLP systems for organizational & corporate security. Author and co-author of more than 10 international & national scientific publications.



Zlatogor Minchev (b. 1978, Burgas, Bulgaria) is an "Associate Professor" (2010) on "Automation and Control" & "Operations Research" at: Institute of ICT & Institute of Mathematics and Informatics, Bulgarian Academy of Sciences; Educational background: PhD on Cybernetics & Robotics (Bulgarian Academy of Sciences, 2006), BSc on Informatics (Veliko Tarnovo University 'St. St. Cyril & Methodius, 2001); IT for Security Department Head (2016); Director of Joint Training Simulation & Analysis Center (2007), organizing and conducting research in the fields of: cybersecurity, future threats analysis, simulated realities validation, robotics & artificial intelligence. Special accent is also given to: human factor response monitoring and stimulation; Distributed Computer Assisted eXercises in mixed cyber-physical realities. Manager & participant in numerous (above 100) research & industrial projects; Author and co-author of a significant number (above 200) of international & national scientific publications.

Rumen Andreev (b. 1955, Sofia, Bulgaria) is an "Associate Professor" (2010) on "Computer Networks & Communications" at: Institute of ICT, Bulgarian Academy of Sciences; Communication Systems & Services Department Head (2010); Educational background: Engineer, Higher Institute of Machine and Electrical Engineering (Technical University), Sofia, Bulgaria, 1975-1980; PhD, Computer Aided Design in Machinery Construction, Higher Institute of Machine and Electrical Engineering (Technical University), Sofia, Bulgaria 1988; Academic Positions: Associate Professor, Head of Department of Communication Systems and Services , Institute of Information and Communication Technologies – Bulgarian Academy of Sciences, (1988-1992); Main research areas: complex systems (ecosystems), communication systems and networks, e-learning; Participant & manager of multiple (above 40) research projects; Author and co-author of a significant number of international & national scientific publications.