Trakia Journal of Sciences, No 4, pp 418-424, 2014

Available online at:
http://www.uni-sz.bg
ISSN 1313-7069 (print)
ISSN 1313-3551 (online)
doi:10.15547/tjs.2014.04.012

Original Contribution

SOFTWARE APPLICATIONS SECURITY

J. Karakaneva*

Department of National and International Security, New Bulgarian University

Abstract
The paper presents some considerations on the security of software. The author reveals several aspects of security in view of new global digital environment. The statement is focused on the need for the incorporation of security requirements throughout the whole software life cycle. There is the suggestion for strong life cycle for secure software. The article describes the efforts of the community in the context of creating a regulation for the development of secure software embodied in the international standard ISO/IEC 27034-1 and the ways of its use by the organizations (The author follows the publication of Reavis Consulting Group, LLC „The emergency of software security standards: ISO/IEC 27034-1:2011", may 2013).

Key words: software security, application security, ISO 27034, cyber security.

INTRODUCTION

In today's virtualized IT world any organization seeking to improve the efficiency of business processes through the introduction of new information technologies. Of course, the software is the component that is the basis of all information processes, and one of the components of information systems, along with the hardware and the human factor.

Meanwhile, the development of the technology of cloud computing creates the opportunity new software to be put in operation in a relatively short time, which gives greater flexibility of information processes in organizations. The traditional model of using software includes purchase and licensing of the necessary software and subsequent maintenance. This scheme increases the overall cost of the introduction of IT in organizations.

Using cloud services allows millions of users to have access to a single instance of the software application. Users pay only for the use of the service. The providers of such services are worried about the legalization of software, and users are free from care management and maintenance of software and licenses. This new reality raises the quality of software products. Due to the involvement of a large number of service providers and consequently a large amount of users new challenges related to security of information in cyberspace and risk management arise. Growing need for new regulatory mechanisms to manage processes and to obey all stakeholders. One approach is the establishment of international standards governing the use of IT and this way to provide the basis for implementation of the strategy and policies in the field of security.

In November 2011, the International Organization for Standardization (ISO) published standard ISO/IEC 27034-1, "Information technology - Security techniques - Application Security", which focuses on the management of software security. This standard is a significant step in the efforts of the IT industry to create secure software and improve risk management through greater transparency of services. The standard is the result of research, implementation, monitoring and analysis of software companies, academic, government and other entities, established the best practices for creating secure software. The leading approach is a placement of security as a priority throughout the whole software life cycle. The result of these practices is not perfect, but more secure software, which can be trusted and to be continuously improved. IT industry can do much

***Correspondence to**: *Juliana Karakaneva, New Bulgarian University, Department of National and International Security*

to increase the chances for adoption of a holistic approach to application security, as prescribed by the standard ISO/IEC 27034-1.

ISO/IEC 27034-1 defines the concepts, frameworks and processes to assist organizations to integrate security within the software development lifecycle. ISO/IEC 27034-1 does not prescribe specific security solutions or technological tools, but provides a methodology for the organizations with regard to the security. It is designed to be compatible with the existing software development lifecycle.

Aspects of Software Security

Need for statutory regulation of software development

Ever increasing use of information technology and the growing threat to the security of information processes lead to increased requirements for the regulation of the IT sector.

Insecure applications affect all stakeholders in virtual space and they have a shared responsibility to improve the reliability of the software, so that the software industry must comply with this reality.

Corporate environment of business

Within the corporate business the organizations are encouraged to develop secure information processes and apply best practices in the field of information system security. The organizations should consider the effect of the application of unprotected software beyond their corporate boundaries. Using software components of unknown origin or uncertified ones to produce new applications poses a serious risk to consumers. To meet customer demand, the industry develops products promptly and don't implement the necessary processes for verification and validation in accordance with the requirements of security, which creates a security risk throughout the supply chain.

Protection of intellectual property and valuable information assets of organizations

For many organizations, intellectual property is the most valuable asset. Intellectual property is a class of asset that consists of creations of the mind or ideas for which property rights are recognized – for example inventions, innovations, projects or data, as well symbols, names, images which can uniquely identify an organization. These assets are embedded in the information systems and frequently are under siege by criminals, competitors, and even foreign nations.

Threats to business intellectual property are more complex and expansive in global space. Threats range from unethical competitors illegally obtaining information, to countries nationalizing intellectual property by use their power to employees stealing and selling these valuable assets, to large-scale counterfeiting by organized criminality. Increased business exposure in emerging economies and advancements in technology have also contributed the growth and complexity of intellectual property threats. Counterfeiting and piracy are two threats that are ordinary in today's business environment and have become the most costly to business and world trade.

Protecting against them should be of permanent concern for organizations looking to maintain their competitive power. The combination of government protections, sound risk management strategies, and corporate oversight is a crucial condition in providing security of valuable assets.

Increase the number of used fixed and mobile IT devices

Several technology companies have made bold predictions that the current 10 billion devices connected to the Internet will soon reach 50 billion or even more [1]. All of these devices depend on the software to function. At the Congress of the Cloud Security Alliance (2012), US Bank CISO Jason Witty presents the importance of software applications for financial services, in the sense that compromised software is a huge risk to the world economy. 93.6% of the total world currency, or $ 212 trillion is virtual and exists only by software [2] , and this indicator explains why the financial services sector traditionally early apply best practices of information security.

Wide application of cloud services

Software as a Service (SaaS) is the future dominant model for the delivery of software, which is significant for many reasons. Organizations will realize financial savings by using cloud-based applications (services to millions of clients simultaneously from a single instance of the software). But the risk of security increases.

Roles in software space

Understanding the consequences of use of unprotected software and making the appropriate decisions require insight into the whole system of production and consumption of software. It is

necessary to pay special attention to the participants and their roles within the virtual cyber system. Many organizations have a dual role – as producers and consumers of software and there is a shared responsibility, because the failures in some of the organizations may have an impact on other stakeholders. There are the following *roles* of cyber participants:

• Users. Everyone is a consumer of software on a personal or business level. Skilled users are able to take the right decisions at different choices when buying or using software. On the other hand large companies have the resources to hire experts for the evaluation of software vulnerabilities and security features.

• Regulators, IT auditors. This category includes internal and external experts who verify conformity with the standards for IT systems.

• Software providers.

- Software Companies, including developers of software tools and application programming interfaces (APIs), which extend the functionality of the software;
- Integrators of software;
- Suppliers who provide software functionality as a service [3]. NIST has defined three basic models of delivery [4]: software as a service (SaaS), platform as a service (PaaS – for rapid application development) and infrastructure as a service (IaaS – operating systems and databases);
- Own internal developers – some organizations develop software for their own use;
- Supply chain – any combination of the foregoing.

There is so called corporate software, which is a product of the development of different manufacturers. Some weakness of a separate module or subsystem can affect the quality of co-operation. Vulnerabilities in particular components are inherited and lead to a general lowering of the security features of the entire software system. This also is valid for use of a set of compatible services in the cloud or compilation of the software components in order to achieve certain functionality, for which there is not sufficient information.

Upstream developer may not have access to the source code, and has only the interface to the service. Usually there is no available information on the security features of software components. The presence of unidentified vulnerabilities in the software can cause later serious damage, such as denial of service, breaches or data loss, compromise of the website and the subsequent loss of confidence by clients and partners of the organization.

Software Life Cycle

It is essential for consumers to obtain and use secure software. One of the main approaches to achieve this goal is to reduce vulnerabilities by testing and elimination of gaps, which is the responsibility of manufacturers. But unless vulnerability assessment, it is important monitoring the supply and maintenance of software, i.e. to ensure security throughout the whole software development life cycle (SDLC). Understanding of the software life cycle is a critical success factor for the implementation and application of the software. In security regard, this means the integration of security attributes throughout the whole life cycle, which includes people, processes and technology.

Since 2004, Microsoft Corporation [5] applied this principle based on the Microsoft Security Development Lifecycle, which includes the idea of embedding security into the development process and implementation. Each phase of the life cycle consists of processes and control mechanisms, allowing the transition to the next phase of development without failures. The framework includes the phase for initial and ongoing security training. Although the adopted configuration is available for use primarily by large companies in developing critical in terms of security of products, it can be used in relatively small projects. Moreover, any software should be developed according to the requirements for reliable operation and performance. Therefore this scheme lifecycle as applied in the development of applications with high security requirements, and in the conventional ones. Microsoft SDL process is made available under the license Creative Commons, allowing each organization to use it for their own software. One of the main benefits for organizations that use a structured life cycle security is the return on investment. Identifying software bugs and potential security issues at the earliest possible stage makes it possible to eliminate these problems with less money than in a later phase.

IBM applies other best practice, so called Agile Software Development Life Cycle [6]. First step is to divide the product or solution into features which need to be developed. If there are new

features identified in the complete product release it again gets planned across iterations. Agile Sprint (iteration) duration depends on the feature to be developed. Every sprint goes through the phases of Requirement, Design, Development and Testing.

- Requirements phase – software requirements are defined.
- Design phase – design of the product/solution is performed. Test team understands the requirements and draws a test plan to proceed with testing of the piece being developed.
- Development phase – developers write source code for solutions and then test unit of the developed functionalities. The test team is involved in writing test cases for functionalities.
- Test phase – the team makes manual testing on the basis of test cases written and also automation testing may be done. The development team is involved in fixing the reported bugs and test team re-verifies it.

Some important advantages of this approach are: early identification of defects in already working modules; use of regressed automated scripts from testing phase to development phase and do not introducing bugs in already existing pieces; identification of requirement or design misses and prevent transferring of bugs to the later stages.

Regardless of many authors suggested similar life cycles [7], here are present the following phases:

- Defining software requirements (of any business process will serve, functional characteristics required, the main security features);
- Development of the software architecture model (modules, relations between them, the critical security database, interfaces, links with other programs);
- Implementation (operating system and development tools);
- Testing:

  - Verification of compliance with the project;
  - Validation functionality, according to the requirements;
  - Modeling threats and checked for reliability and stability under attacks;

- Accreditation the software for intended purpose;
- Planning response to events and incidents in security in operation;
- Decommissioning and storage of data.

Proposal for stronger requirements

The organization decides how to embed security in the software life cycle depending on the level of security they require the business processes. Undoubtedly for military, governmental, financial or critical infrastructure organizations the security has high priority. In these cases a *strong* life cycle for software applications is appropriate. Our proposition is to apply process of verification, validation and accreditation well known from modeling and simulation life cycle [8].

Verification is the process of determining that a software implementation and its associated data[1] accurately represent the developer's conceptual description and specifications.

Validation is the process of determining the degree to which software and its associated data are an accurate representation of the real world from the perspective of the intended uses of the software.

Accreditation is the official certification that software and its associated data are acceptable for use for a specific purpose. Accreditation criteria are defined as a set of standards that particular software must meet to be accredited for a specific purpose. Accreditation authority is the organization or individual responsible to approve the use software, and their associated data for a particular application.

This kind of life cycle ensures high protection of software against the threats and attacks during the operation and required level of security. But there are several problems in this process:

- Only large organization can allocate resources for implementation the process of VV&A;
- Software manufacturers want to quickly put new software in operation and reduce life cycle;
- The process requires the development of specific standards and certified laboratories;
- Trained personnel is necessary to conduct the tests;

[1]Data verification and validation is the process of verifying the internal consistency and correctness of data and validating that it represents real-world entities appropriate for its intended purpose or an expected range of purposes.

- Time is prolonged in implementation of the software in operation.

So the secure software has its price, but protects the valuable assets of the organization against attacks in virtual space. The organization must decide about the right approach to ensure an acceptable level of security.

Information Security Management through Software Security

Industry of information security is in the process of evolution and evolves with the raising technology and new customer requirements. The need to implement the most successful approaches and tools for protection and ensuring the security in cyberspace changes the practice in this area. Some of the important new steps are: information sharing about events and incidents in security and exchange the countermeasures against the attacks between stakeholders. For example, the organization known as the Cloud Security Alliance [9] started initiative for service providers allowing them to publish their security practices in a public register CSA Security Trust and Assurance Registry.

The most important decision in support the security area is the establishment of international standards for regulation of global protection of information security. ISO/IEC SC27 is the group that has developed several other widely used information security standards, including ISO/IEC 27001 (Requirements for information security management systems), 27002 (Code of practice for information security management), and 27005 (Information security risk management). ISO/IEC SC27 is globally recognized as the key standards development organization for information security management practices, and its work is commonly cited and referenced by laws, regulations, and other standards around the world.

The globally recognized standard for certification of security best practices is the ISO/IEC 27001 [10] and many organizations join this community applying the general requirements for information security management systems.

Although not all industries have a clear need to have their information security program externally certified via ISO/IEC 27001, most enterprises are familiar with its principles and have aligned their own ISMS with its code of practice, which is separately described in ISO/IEC 27002, "Code of practice for information security management" [11].

ISO/IEC 27001 gives a systematic approach to information security in general, using risk management and the Plan-Do-Check-Act methodology as its quality assurance model. If an organization has significant software development activities, it would likely seek to include its development division within its scope of certification to build trust in its secure software development program. Application security requires its own standardized frameworks, methodologies, and processes to achieve its goals.

Main guidelines of ISO/IEC 27034-1

ISO/IEC 27034-1 [12] was officially released in 2011 and provides an overview of application security concepts as well as the framework and processes that are needed to operate a comprehensive application security program.

The key principles of the standard are as follows:

A holistic view of application security

A valuable contribution of ISO/IEC 27034-1 in the area of definitions is to encourage a holistic view of application security. Securing software should be viewed in a broad context that includes software development considerations but also the business and regulatory context as well as other external factors that can affect overall security of the application.

Application security requirements

An understanding of risk and the ability to employ this knowledge via risk assessments is crucial to the ability to properly define the appropriate security requirements for any application. An organization's ISMS systematically governs information security risk for the enterprise, including that of the application security program.

Frameworks

These basic ideas have been implemented by two frameworks. Implementation of these flexible frameworks is intended to help organizations integrate security seamlessly throughout their applications' lifecycles. The reference model is a guideline of organization in order to construct own software life cycle.

- Organizational Normative Framework (ONF). The ONF is a framework of so-called containers for all components of application security best practices of the organization. These containers include:

Business context, including all application security policies, standards, and best practices adopted by the organization;

Regulatory context, including all standards, laws, or regulations that affect application security;
Technological context, including required and available technologies that are applicable to application security.

Application specifications repository, which documents the organization's IT functional requirements and the solutions that are appropriate to address these requirements.

Roles, responsibilities, and qualifications, which define the different actors in an organization, related to the IT applications. This container will include a wide range of job titles and duties aside from the developer.
Application security control (ASC) library, which contains the approved controls that are necessary to protect an application based on the identified threats, the context, and the targeted level of trust.

Processes, related to application security.

- Application Normative Framework (ANF). The ANF is derivative of the ONF and is created for a single specific application. The ANF maintains the applicable portions of the ONF that are needed to enable that specific application to achieve the required level of security – the targeted level of trust. Because a typical organization will have several applications to secure, there will be a one-to-many relationship between one ONF and many ANFs.

ISO/IEC 27034-1 defines an application security management process (ASMP) to manage and maintain each ANF. The ASMP is performed in five steps:
1. Specifying the application requirements and environment
2. Assessing application security risks
3. Creating and maintaining the Application Normative Framework
4. Implementation and operating the application
5. Auditing the security of the application
Through all ANF processes of software development the organization collects new knowledge and creates Application Security Control Library. This way the standard gives bidirectional process to build a continuous improvement loop, so that every application being secured ensures the organization gains the full benefit from examination, tools, and capabilities. By combining two frameworks the organization achieves two goals - securing every single application during ANF process and returning the obtained knowledge towards ONF process in order to address the application security in the future.

Compliance with ISO/IEC 27034-1
Following ISO/IEC 27034-1, the business has to put into effect the security of application by ONF methodology. Senior management and IT business unit need to provide executive support for application security best practices. The business stakeholders must take into account the quality of the software and the consequences of non-secure applications as a factor in their risk-based decision making.

Companies that develop software applications should adopt and implement ISO/IEC 27034-1 within the context of their system for information security management and risk management program. The use of the standard will assist to assess the accordance of SDLC with best practices in security.

Encourage transparency within the global software environment
Organizations that are enterprise consumers should align with ISO/IEC 27034-1 as a part of their software vendor management program. It is critical to ensure that supply chain software companies provide secure software for which they are responsible and they have application security programs. Every software package must be provided with complete documentation including the security features. Consumers should require transparency in the documentation of secure development lifecycle programs and should also acknowledge software producers who fulfill these requirements.

Leadership of IT management
IT management personnel are responsible for raising awareness of security in the high echelon of the organization. IT management personnel is responsible to cultivate security awareness in organization Chef Information System Officers have a responsibility and a leadership role in assuring their software suppliers are aware of ISO/IEC 27034-1. They should establish the security practice within the organization SDLC and should track the software procurement. They should also emphasize that international standard ISO/IEC 27034-1 assists using risk-based

methodologies to achieve a targeted level of trust.

Role of regulatory bodies

IT audits community has a responsibility to apply ISO/IEC 27034-1 and its long-term implementation in their assurance activities. These groups should also support the transparency in governance of security area and development practices within software companies.

Software experts' engagement

The community of IT experts in security area has to engage with applying of ISO/IEC 27034-1 and to map it within existing tools, processes, and frameworks in organizations. Doing so they will make their own suggestions on the future versions of ISO/IEC 27034-1 like a container of best practices in order to meet the needs of the secure software systems.

CONCLUSIONS

Non-secure applications impact all participants of cyber space and stakeholders have a shared responsibility to improve the trustworthiness of software. Software companies must treat every existing and under-development application as a security risk until it is proven otherwise, because of the risk which existing vulnerabilities can pose to the business. No single tool will be a miracle to make all software secure, because the legacy code in use is extremely vast. Several tools do help developers and code reviewers to assess applications security and quickly identify the most potentially damaging vulnerabilities. The companies able to efficiently and effectively integrate the analysis into their software development lifecycle practices will not only improve their own security state but will achieve substantial business benefits for themselves and all those that rely on their software.

The entire community – developers, partners, and customers – have to work together to assure that the principles of ISO/IEC 27034-1 for secure software development become as wide-spread as software itself.

REFERENCES

1. http://readwrite.com/2011/07/17/cisco_50_billion_things_on_the_internet_by_2020.
2. CSA Congress keynote by Jason Witty https://cloudsecurityalliance.org/wp-content/uploads/2013/01/2012-CSA-CloudCongress-Witty.pdf.
3. CIO.com: Long live SOA in the Cloud Era. http://www.cio.com/article/2394821/cloud-computing/long-live-soa-in-the-cloud-era.html
4. NIST Special Publication 800-145 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
5. Microsoft SDL Progress Report: http://www.microsoft.com/en-us/download/details.aspx?id=14107
6. Kumar Saraya, S., A Process for Reducing Defect Risks from Development to Test phase in Agile Software Development Life Cycle, 2013**.**
7. http://www.veracode.com/security/software-development-lifecycle
8. Department of Defense INSTRUCTION**,** DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A), 2009.
9. CSA Security, Trust and Assurance Registry, https://cloudsecurityalliance.org/star/
10. ISO/IEC 27001:2013, „Information technology – Security techniques – Information security management systems — Requirements".
11. ISO/IEC 27002:2013, „Information technology – Security techniques – Code of practice for information security management".
12. ISO/IEC 27034-1:2013, "Information technology – Security techniques – Application security", 2011.