Information Security Risk Management in a World of Services

Vincent Lalanne[1] Manuel Munier[1] Alban Gabillon[2]

[1]**LIUPPA** (Computer science Laboratory) UPPA - University of Pau, Pau, France

[2]**GePaSud** French Polynesia University, Tahiti, France

2013 ASE/IEEE PASSAT

International conference on Privacy, Security, Risk and Trust

September 8th - 14th, 2013 - Washington D.C., USA

ASE Academy of Science and Engineering

IEEE computer society

This paper:
Information Security Risk Management in a World of Services

- Service Oriented Architectures (SOA) offer new opportunities for the interconnection of systems
- Opening the Information System to the "World" is not insignificant in terms of security
- New technologies (eg cloud) have introduced new vulnerabilities and therefore new risks

This paper

Information Security Risk Management in a World of Services

⇒ We propose an approach for risk management which is based on the ISO/IEC 27005:2011 standard

  ⇝ development of this standard to take into account the type "service" as web services and cloud services

⇒ We introduce a new security criterion: **controllability**

  ⇝ A world of services is more a relationship between customer and supplier, where notions of trust, accountability, traceability and governance are developed.

Outline

Information Security Risk Management in a World of Services

Table of contents

Information Security Risk Management in a World of Services

Information System

- First information systems used in companies operates in autarky, that is to say closed to the outside world and only supplied by the internal data from the enterprise.
- Connecting to other systems quickly emerged, thus increasing the amount of information available, outsourcing some processes and offering new services to both employees (working at home, nomadic users,...) and customers (web portals, information flow,...).
- The increasing use of mobile devices, smartphones or tablets in the professional world (BYOD[1]) also introduces new risks that companies must face.

[1] BYOD: Bring Your Own Device

Table of contents

Information Security Risk Management in a World of Services

A World of Services

- Interconnections between information systems via web services can be carried out either on private infrastructures or through the Internet.
- Cloud technology involves many services in the field of computing, storage, information processing,...
  - ⇝ Infrastructure as a Service (IaaS)
  - ⇝ Platform as a Service (PaaS)
  - ⇝ Software as a Service (SaaS)
  - ⇝ Monitoring as a Service (MaaS)
  - ⇝ Communication as a Service (CaaS)
  - ⇝ Data as a Service (DaaS)
  - ⇝ InFormation as a Service (FaaS),...
  - ⇝ ... the XaaS (Anything as a Service) is born and include all services directly accessible from the Internet and that grow on the business model of cloud computing.

REST (REpresentational State Tranfert)

Web Services Security

- REST [2] is a design pattern for implementing connected systems.
- RESTful architecture meets several principles:
  - Applications are client-server,
  - requests are stateless,
  - clients and servers use a uniform interface; all resources are accessed through well defined methods like HTTP, GET, POST, PUT, DELETE, HEAD and OPTIONS.
  - Clients access to named resources;
  - the system understands named resources using URLs such as HTTP URLs (but not only limited to HTTP URLs).

[2] R. T. Fielding and R. N. Taylor, "Principled design of the modern web architecture," in Proceedings of the 22nd international conference on Software engineering. ACM, 2000,

SOAP (Simple Object Access Protocol)

Web Services Security

- SOAP [3] establishes a general framework for exchanging complex data in XML.
- SOAP does not depend on the programming languages or the operating system on which it is implemented.
- A SOAP message is a unidirectional transmission between SOAP nodes, from a SOAP sender to a SOAP receiver.
- SOAP messages are supposed to be combined by applications to implement more complex sequences of interactions: from the basic question and answer model to multiple bidirectional exchanges for "conversational" scenarios.
- A SOAP message is an XML document constituted by an Envelope containing a Header (optional) and a Body (the message).

[3] W3C, "SOAP version 1.2,"

Security measures I

Over the SOAP protocol, we can list a number of existing security measures to strengthen security of infrastructures that using web services:

- WS-Trust: specification for the generation, renewal and validation of security tokens,
- WS-SecureConversation: creation and sharing security contexts,
- WS-Federation: mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication
- WS-Authorization: expression of authorizations
- WS-Policy: flexible and extensible grammar for expressing the capabilities, requirements and general characteristics of entities (customers or suppliers)

Security measures II

- WS-Privacy: model to indicate how confidentiality requirements and practices related to private data is transmitted between organizations

Other specifications concern more specifically the phases of authentication and authorization.

- SAML[4] specification defines a framework for exchanging authentication information and authorization between business partners.
- XACML[5] defines a language for access control, rule propagation and administration of security policy for information systems.

[4] SAML: Security Assertion Markup Language
[5] XACML: XML Access Control Markup Language

Table of contents

Information Security Risk Management in a World of Services

Why a Standard for Information Security ?

- Existing methods for ensuring information security can not be a trust mark for the overall security of the company, because it is often developed internally and difficult to change (long term support ?).
- To meet the need for overall confidence in the digital economy, work has been initiated to establish international standards for information security.
- Since a decade, companies having many data exchanges with other companies (national or international) or with many partners and customers, have experienced the need to agree on standards to secure information and exchange processes. It is precisely this goal that led to the creation of the ISO/IEC 27005 standard.
- ISO/IEC 27005 aims to establish a trust mark for the overall information security within enterprises.

Standard or Method ? I

- A standard is defined as a document based on a consensus covering a broad industrial or economic interest and established by a voluntary process.
- In contrast, a method is an effective way to achieve a desired and accurate result. But a method does not include the notion of document, neither the concept of consensus.
- We should not oppose standards and methods, but rather combine them: a method will be the "tool" used to meet a standard.

Standard or Method ? II

- To effectively implement the ISO/IEC 27005 standard, we can thus rely on a risk management method as:
  - ⇝ CRAMM: **C**CTA (Central Computer and Telecommunications Agency) **R**isk **A**nalysis and **M**anagement **M**ethod (United Kingdom),
  - ⇝ Octave [6] (United States),
  - ⇝ EBIOS: **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité (expression of needs and identification of security objectives) (France).

[6] C. Alberts and A. Dorofee, "An introduction to the octave method" Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.

History

Introduction to the ISO/IEC 27005:2011 Standard

- 1995: BSI[7] publishes BS 7799 standard, it focuses on ten major chapters that list the actions (one hundred) that can be taken in relation to information security.
- 2000: ISO officially adopts it under the reference ISO 17799 (now known as ISO 27002).
- 2008: ISO 27005 is published, its purpose is to provide guidelines for information security risk management.
- 2011: A new version of ISO 27005 standard appeared.

[7] BSI: British Standards Institution

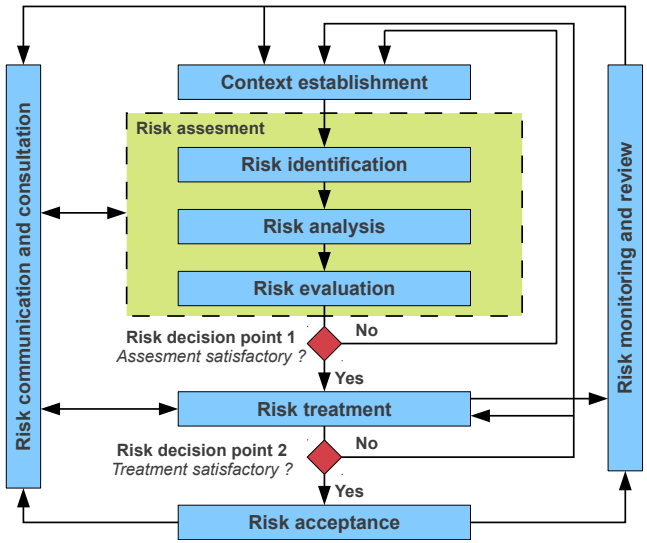
ISO/IEC 27005:2011 Standard I

Introduction to the ISO/IEC 27005:2011 Standard

- ISO/IEC 27005:2011 gives recommendations and therefore it quite often uses the conditional
- The first five chapters of the standard are very short and deal only with generalities.
- Clause 6 gives an overview of the information security risk management process

ISO/IEC 27005:2011 Standard II

Introduction to the ISO/IEC 27005:2011 Standard



- The information security risk management process consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication and consultation (Clause 11), and risk monitoring and review (Clause 12).

Observations

The difficulties encountered in risk management in distributed information systems are intrinsically linked to the SOA model.

- Such a "logical" architecture relates at the same time hardware aspects, software. Although ISO/IEC 27005 can already take these aspects into account in the study boundaries, it treats them individually: datacenters, network connections, computers, applications,... Moreover, existing technical solutions to improve IS security also address these points individually: backup servers, clusters, redundant links, encryption tools, system administration, application monitoring,...

- But now a world of services is not limited to link interconnected systems, it is more a relationship between customer and supplier, where notions of trust, accountability, traceability and governance are developed.

Table of contents

Information Security Risk Management in a World of Services

Context establishment
Conduct of ISO/IEC 27005 Standard

- We do not deal with the study of securing the web services themselves we rather propose to study the impact of using a SOA on the information system security from the point of view of the risks related to information security.
- Our work concerns the interconnection of information systems (broadly defined) through the use of web services. We do not focus on the "internal" security of these web services (eg injection of erroneous parameters), but rather on the impact of a "failure" of a web service on the Information System.

Identification of assets

Conduct of ISO/IEC 27005 Standard

In this context, we are led to consider two types of assets:

- Web Services themselves: input and output data flows, business processes they implement,...
- Underlying communications infrastructure: systems (computers and OS), network, software platforms (eg SOAP implementation, servlet container),...

Identification of threats

Conduct of ISO/IEC 27005 Standard

Within the meaning of ISO standards, a threat is *"a potential cause of an incident, that may result in harm of systems and organization"*. Threats may have natural or human origin, and could be accidental or deliberate. A risk is *"the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization; it is measured in terms of a combination of the probability of occurrence of an event and its consequence"*.

- an incident on the network causes malfunctions (excessive delays, loss of connection)
- a malicious person intercepts messages and forge new posts to harm the IS and/or access certain information
- a software error (accidental or deliberate) on a WS causes the sending of erroneous results

Identification of vulnerabilities I

Conduct of ISO/IEC 27005 Standard

- Vulnerability is **"a weakness in the information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source"**.
- Our research activities are at a higher level of granularity: we focus on the security of the information itself:
  - content structure,
  - chain of production and consumption,
  - economic and legal issues related to the information.
- If you look at the cycle of information processing (storage, processing, transport) as such, it is certain that many vulnerabilities and threats are emerging with the use of "cloud" services.

Identification of vulnerabilities II

Conduct of ISO/IEC 27005 Standard

- Thus, we can classify these vulnerabilities according to several categories:

- **Quality of Service**
- **The location of data and processing**
- **Loss of control of information**
  - **incident** at the service provider
  - **Reversibility**: it is supposed to allow the client to repossess his data at any time without justification.
  - **Termination of the contract**: physical erasure of data is rarely complete.
- **Information ownership**
- **The type of information**

Identification of consequences I

Conduct of ISO/IEC 27005 Standard

From the previous list of vulnerabilities (not exhaustive) we can now present some basic scenarios illustrating the occurrence of a threat that exploits a vulnerability in a service with its impact on the information system.

- **Quality of Service**:The service provider does not fulfill the service by itself; it is a broker with service subcontractors. In case of litigation or digital forensics the issues regarding the quality of the services and/or responsibilities are very difficult to determine.

- **Data stored in a foreign country**: However, some businesses do not like the ability of a country to get access to their data via the court system, for example, an European customer might be concerned about using Cloud Computing system in the United States given the USA PATRIOT Act and PRISM (since 2007 and revealed in june 2013 by Edward Snowden).

Identification of consequences II

Conduct of ISO/IEC 27005 Standard

- **Prohibited or copyrighted informations**: when sharing a service that is not looking at the origin of the data it stores, the service can be closed overnight eg. Megaupload 2012, resulting in a direct loss of data for the friendly customers of the law.

- **The provider has financial difficulties**: the supplier fails and stops the services it provides. It can also claim money to restore your data (eg 2e2.com 2013).

- **Data recovery**: closing procedures of a service, such as at the end of a contract, should provide the ability to retrieve data (reversibility) but also ensure their final removal on provider's servers (physical erasure of data).

Evolution of ISO/IEC 27005 Standard Towards Services I

We propose to add in Annex D of the ISO/IEC 27005:2011 standard a new type named "service".

Type	Examples of vulnerabilities	Examples of threats
Hardware	...	...
Software	...	...
Network	...	...
Service	Lack of long term support from service provider	Service no longer available
	Unknown life cycle and update policies from service provider	Unexpected change of the service interface
	Unknown country to host services	Spying, data theft
	Failure to comply with the laws in force	Service no longer available
	Provider goes bankrupt	Service no longer available
	Laws on privacy differ in the country of use	Loss of confidentiality
	Laws on information security are less restrictive	Spying, data theft
	Laws on information security are more restrictive	Service no longer available
	Inadequate Service Level Agreement	Breach of maintainability of the IS
	Lack of data recovery procedure	Breach of maintainability of the IS
	Lack of reversibility (migration, interoperability)	Breach of maintainability of the IS
	Lack of data erasure at the end of the contract	Data theft, unauthorized use
	Lack of WS metadata security	Tampering with the web service
	Possible multiple requests to the WS	Identity spoofing
	Lack of traceability of the service provided	Breach of trustworthiness of information
Personnel	...	...
Site	...	...
Organization	...	...

TABLE I. A NEW TYPE "SERVICE" IN ANNEX D OF THE ISO/IEC 27005:2011 STANDARD

Evolution of ISO/IEC 27005 Standard Towards Services II

- As explained in this paper, our work concerns information security as a whole: from contents to economic and legal issues.
- Vulnerabilities bring simple questions that are at the heart of every service user and allow it to guarantee some "**Controllability**" about his data:
  - How do I know where is my data ?
  - How do I know who can access my data ?
  - Can I easily change provider ?
  - In what country my data is stored ?
  - My data is it legal in the country where it is stored ?
  - Does my provider impose respect for the intellectual property to all its customers ?

Evolution of ISO/IEC 27005 Standard Towards Services III

Thus, the concept of "**controllability**" appears fundamental in the design of information systems using "services".
It is quite possible to define a fourth security criterion specific to services, in addition to the three basic criteria CIA:

1. **Confidentiality**: it prevents the unauthorized disclosure of information (eg illegal read access)
2. **Integrity**: it guarantees the accuracy, completeness, validity and stability of information
3. **Availability**: it ensures continuity of service and system performance
4. **Controllability**: it ensures complete control over services used

Table of contents

Information Security Risk Management in a World of Services

Related Work I

- Information exchange between systems and particularly in the cloud introduce new risks with regard to information system security. As pointed out Pieters and al, there are two methods to remedy: trust the service provider or implement technical mechanisms to compensate for a trust worthy supplier.
- First to compensate the lack of trust in a service it's necessary to put in place mechanisms that enable secure information exchange between systems. Hamlen and al,discuss security issues for cloud computing and present a layered framework for secured cloud storage. They focus on essential aspects: how to store data in foreign machines, querying encrypted data and secure this queries.

Related Work II

- Accountability as seen from a holistic point of view, covering legal, socio-economic, regulatory and technical aspects is presented in Pearson and al. That European project named A4Cloud aims at four objects which tackles accountability developing tools that:
  1. enable cloud service providers to give their users appropriate control and transparency over how their data is used,
  2. enable cloud end users to make choices about how cloud service provider may be use,
  3. monitor and check compliance with user's expectation, business policies and regulations,
  4. develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services.

Related Work III

- In the **European Network and Information Security Agency** (ENISA) a Preparatory Action entitled "Trust and privacy in the Future Internet" covers in one work package identity, accountability and trust in the Future Internet. The objective is to study security models of electronic services and their performance in highly distributed environments, such as today's Internet. Furthermore, ENISA investigates various ways of assuring privacy and accountability on the Internet, reviewing the most prominent methods used, studying their mapping to the underlying architectures and assessing their level of effectiveness and performance. ENISA also works towards the development of recommendations on the use of specific service models in given environments and architectures.

Table of contents

Information Security Risk Management in a World of Services

Conclusion and Future Work I

- SOA models including cloud services are increasingly used because of the benefits they provide.
- From the point of view of information security risk management, these technologies introduce new vulnerabilities with regard to the use of external services that we can not control, responsibilities related to the provision of service,...
- There are solutions to secure these exchanges and design "reliable" web services.
- Our work is complementary to these solutions because we operate at the level of information security within the meaning of the ISO/IEC 27005:2011 standard.

Conclusion and Future Work II

- Our goal is to refine the process of risk management to the specificities of services in an SOA by taking into account the information in its entirety, including socio-economic and legal aspects.
- We therefore suggest to extend the ISO/IEC 27005:2011 standard to include consideration of services (web services, cloud) in the risk assessment of information security.
- Having identified a number of scenarios that can not be avoided through the existing security mechanisms, the second phase of our work is to propose a security model for communications between IS.
- To achieve this goal, we consider a usage control oriented approach, as we have already experienced in our previous work on intelligent documents (cf. *Enterprise Digital Right Management*).

Conclusion and Future Work III

- The use of metadata for traceability of communications (via these services) will also allow us to compute indicators that can be used to monitor the IS.
- Enhancing the importance of providing more transparency and control to processes mediated by the cloud and taking into account that data is dynamic due to the complex responsibility chains, we also propose as a perspective an approach based on preventive, detective and corrective accountability methods.

Vincent Lalanne, Manuel Munier, Alban Gabillon

Information Security Risk Management in a World of Services

Thank you for your attention.

vincent.lalanne@univ-pau.fr

http://www.univ-pau.fr/

http://www.upf.pf/