oktober 2009 nummer 6

INFORMATIEBEVEILIGING

Cybercriminaliteit kost bedrijfsleven en overheid handenvol geld

De Leidraad voor de uitwisseling van gevoelige informatie van NAVI

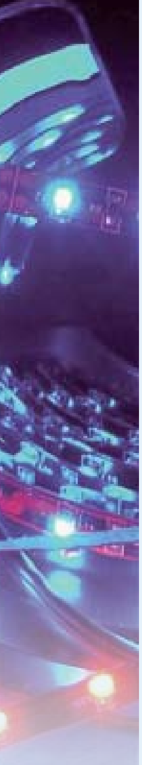
Cybercrime trendrapport: geen verbetering van de veiligheid van internet

Voorkom schijnveiligheid door een veilig ontwerp

DEMO architectuur met security

PvIB
Platform voor
InformatieBeveiliging

ib



Use of DEMO as a methodology for business and ICT security alignment

Auteur: Yuri Bobbert > Yuri Bobbert is Consulting Partner at B-Able, certified DEMO professional. Hij is per email bereikbaar via yuri.bobbert@b-able.nl. Co-author: Joop de Jong, Lector Extended Enterprise studies at Utrecht University of Applied Sciences and member of the Demo board.

In search of finding stronger methods to design a secure enterprise, DEMO[1] is underexposed. DEMO is a widely adopted international standard for designing and engineering 'extended enterprises'. The notation 'extended' indicates the broad variety of social interaction and interoperatibility between enterprises to accomplish a mutual benefit. Enterprises work together on all kinds of layers within the organization and therefore they cope with more and more extended inter(trans)actions that make use of information technologies –like the internet- to exchange business critical information. The exchange of critical information via the internet and the possible impact this may have on the confidentiality, integrity and availability of this information is rather unknown. The problem of the unawareness of security breaches that might occur during the information exchange between enterprises emphasizes the urge of examining the three mentioned areas of concern at the start of the design phase. In our opinion, it has to be embedded into the theory of design.

The objective of this article is to determine the security aspects which are unique for each DEMO layer as well as the principles for implementing secure enterprises.

Background

To make this rather technology orientated paper readable for 'business' audience (target area) we would like to discuss a case about a fictional hospital. By using this case, business people have to abstract from all the details of this specific case to a more general way of working concerning exchanging data with third parties.

In particular, the effects of not exchanging data securely are exhibited. I chose the hospital case because every Dutch citizen was recently requested to authorize access rights to his or her medical records.

The main objective behind this request is to serve better healthcare in the Netherlands. With the electronic patient database (EPD) developments in mind and knowing that the data exchange infrastructure is far from ready to exchange this EPD securely, there was enough reason to examine this subject. Another reason why I chose this hospital case is due to the fact that commercial companies are developing health care applications (e.g. Google Health). With these applications it is possible to view records and exchange medical files. New web[2] technologies not only make it possible to exchange between hospitals but also between commercial companies, and even countries with other social ethics. For involving third parties into your own business process we consistently use the term 'extended enterprise'. So the example of a hospital that makes use of web technologies to exchange confidential medical records can be considered as an example of the extended enterprise.

The social impact of technology so far ahead of what we morally may want, makes it even more necessary to examine and to present a well considered way of modeling secure extended enterprises. The main reason for examining this topic is to find out if DEMO is suitable for the design of a secure extended enterprise.

What is DEMO?

DEMO is developed by Prof. Dr. Ir. J.L.G. Dietz at Delft University. DEMO has proven itself to be an effective methodology of decomposing the enterprise based upon the ψ-theory. The Greek letter is pronounced as PSI and stands for Performance in Social Interaction. This is the basic paradigm of this theory: the performance of the business in relation to the social interaction with itself and other systems. DEMO distinguishes three layers of critical essence: the business layer, the information layer and the data layer.

The business layer is the essential layer for enterprises to communicate and interact to establish business critical results. This layer consists of actors who initiate unique actions that lead to unique results. On this layer actors can interact with other social entities (actors) from other enterprises. For example a surgeon in hospital A requires a medical record to treat a just brought in car-crash patient whose medical records have been recorded in Hospital B. The treatment of this patient is the core business of the hospital and the responsible and competent actor who is authorized by hospital A is the surgeon (actor). The treatment of the patient leads to new and unique facts.

The information layer is the intermediate layer between business and data. The business actors need information to conduct their production acts. The information is the result of interpreting

[1] DEMO Design and Engineering Methodology for Organizations (http://www.demo.nl).

[2] In common literature this advanced way of exchanging data via the internet is called WEB 2.0.

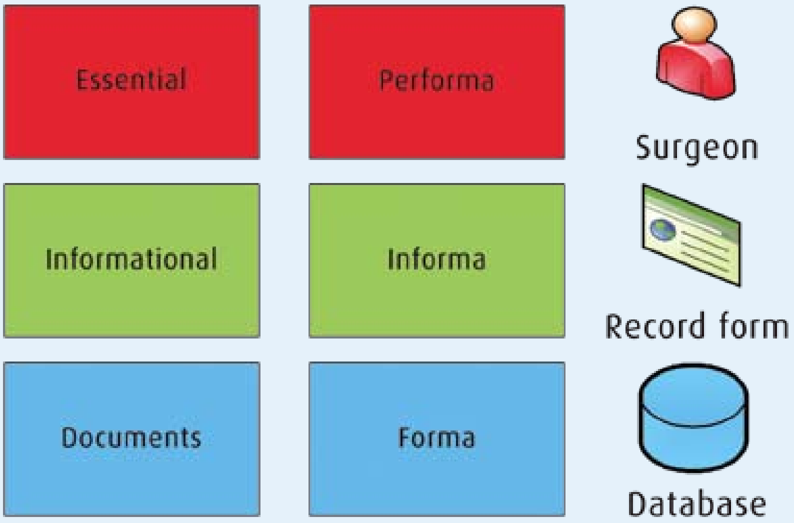


Figure 1: The three DEMO layers and their function

the data. The data initially is extracted from the data layer and is computed, reasoned, etcetera, by the information layer before it is offered to the business layer. In our example the surgeon reads the medical record (EPD) by use of information technology. The record is presented in a certain user interface. Before the data reaches the surgeon certain compatibility algorithms (protocol hand-shakes) need to be exchanged between both systems before the surgeon has privileged access to the patient's private records.

The data layer stores, copies or destroys all kind of documents (data). This layer distinguishes from the information layer in that it only concerns the form (forma) of the data and that it is not concerned in the content (informa) of the data. In the hospital case the surgeon approaches the medical records of the patient via the information layer. The medical records are stored in the data layer as static information in bits and bytes. This information could be blood type information and statistics or medical history to effectively threat the car-crash patient with the right type of blood and the right medication.

When we extend this data exchange to other enterprises the surgeon we had previously might need to extract several forms of data from several other enterprises.

Why DEMO-transactions?

Demo is used to visualize which layers within the organization serve the business function (conducting the business transactions), the information function (delivering information and storing original actions), and the data function (storing, retrieving and transmitting data that corresponds with original and derived actions). For each layer it has to be determined which transactions are critical and which security aspects are critical. For determining if security principles are suitable to embed into DEMO in this article we focus on the applicability to the Business and the Information layer only. Our special attention is to discuss where in the different DEMO models for both layers we have to introduce these principles. To determine which security principle to use in DEMO, we build on the three basic security principles Confidentiality, Integrity and Availability, CIA in short. I used these three basic principles to map them over the several DEMO models and derive them subsequently into principle scenarios.

On the business function (Performa) contextual influences, like corporate governance, and organizational political influences, like IT governance and security principles, have impact on business processes and might harm the confidentiality, integrity and availability of business transactions. By making use of the Transaction Result Table (TRT) we can quickly determine what breaches can occur on a specific business transaction and what their impact could be on the result.

With the help of the Information Use Table (IUT) and the Process Structure Diagram (PSD) we can determine where in the business transaction certain information is required. On these IUT and PSD the CIA principles are mapped to determine where security breaches might influence the transaction. In this example medical files can only be accessed by an authorized doctor, unauthorized individuals are not allowed to access these files. The identification and the claim to authorization are typical security aspects which have to be dealt with by actors at the Informa layer in the organization. By means of the data layer, the data that corresponds with original actions is stored to serve the above lying information layer. By separating static data (data at rest) from dynamic information (in motion) you can decide what CIA breaches can occur and what measures are required to mitigate risk or damage. For example you could store medical records at a Trusted Third Party on a high available storage cluster with strict separation of duties or you could store them in the cloud at Google.com. Both are ways to store data but with different CIA perspectives, the DEMO theory is a powerful method to distinguish data formats (Forma) and to determine where and when to implement certain security principles.

Because DEMO addresses business, information and data layers of the organization the DEMO theory ought to be more accepted across the enterprise departments. It provides insights in all organizational layers and therefore in possible information security issues. By

Initiator	Transaction	Result	Executor
CA01 Patient	T01 Treatment of Patient P	R01 Treatment of patient P has been completed	CA00 Treatment Handler
CA00 Treatment Handler	T02 Treatment by Medical Expert	R02 Treatment by Expert has been completed	A03 Expert
CA00 Treatment Handler	T03 Approve Medical File View	R03 File View has been approved	CA01 Patient

addressing each layer and making use of the SDEMO checklist (explained later on) it makes IT security 'readable' and therefore acceptable for business as well as IT people. It helps business and IT align by achieving mutual goals.

Understanding security breaches and possible risks help create awareness and is a necessity when it comes to allocating IT investment.

From DEMO transactions to security principles

To determine which principles to implement per layer we need to breakdown from ontology to construction. Dietz introduced DEMO and mainly focused on the business layer of the enterprise. De Jong focuses more in detail on distinguishing between information and data and how to construct architectural principles. When we introduce security principles in the design process of the extended enterprise it is necessary to address these principles during the design of these information (I) and data (D) layers. De Jong calls this the design of the D and I-organization. Based on the work of De Jong I will elaborate on some security principles by using the hospital case as an example of the extended enterprise.
To fully understand the essential need for DEMO I have followed the several DEMO modeling methods and made use of the basic notations[3]. Starting off with the Transaction Result Table where we state the essential transactions and their results (Facts).

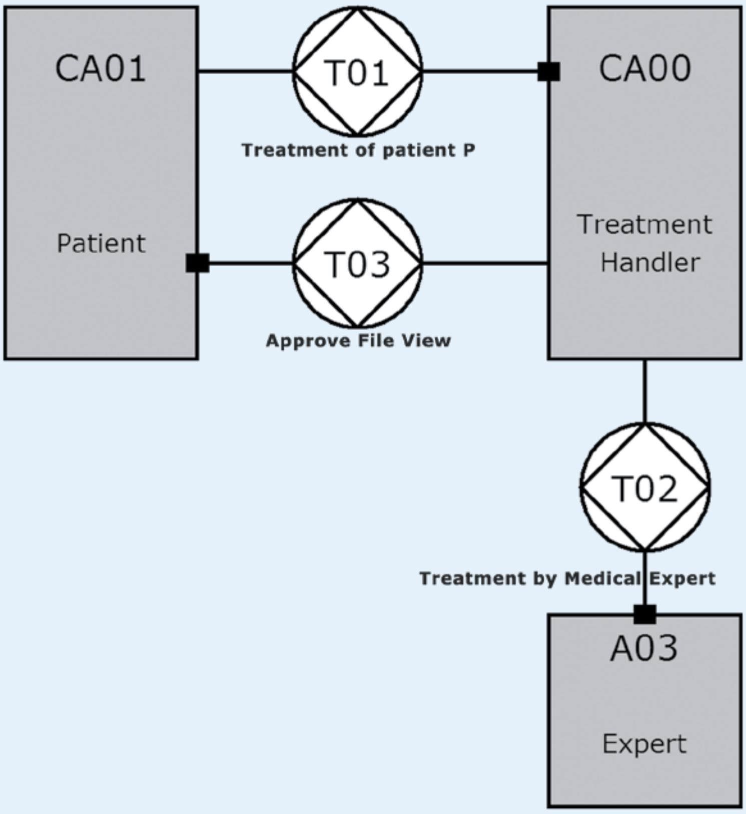


Figure 2: Global Actor Transaction Diagram Hospital Case (ATD)

After the TRT we graphically model these transactions and actors in a Global Actor Transaction Diagram (figure 2).

In figure 3 the ATD is displayed, with Production Bank 'Medical File'. In this case the collective name for EPD and Production Bank is 'Security principles DB'. This is the external source where the hospital gets its security policy (best practices) information from.
It is necessary to determine where in DEMO security principles have to be introduced. Therefore it is important to distinguish the two actor roles in a basic transaction state that a specific transaction is in.
The requester is called the initiator and the deliverer is called the executor. The basic transaction pattern within DEMO is distinguished in three phases. The Order phase, Execution phase, Result phase. These OER phases are detailed by designing the transaction pattern according to the DEMO Process Structure Diagram (PSD), displayed in figure 4.

After detailing the transactions in DEMO we need to distinguish the variety of security threats that might arise during transactions. I therefore introduce a Secure Demo checklist (SDEMO) which can be used per layer of the organization to determine security measures.

From security principles to security investments

The DEMO Product Structure Diagram (PSD) is limited to the business layer. That means that the Security Code of Practice triad of Confidentiality, Integrity and Availability is only applicable for the business layer. The focus on the business layer neglects the layer where most of the CIA breaches arise.

[3] For limitation purposes we narrowed down the number of Hospital Transactions to the basics.

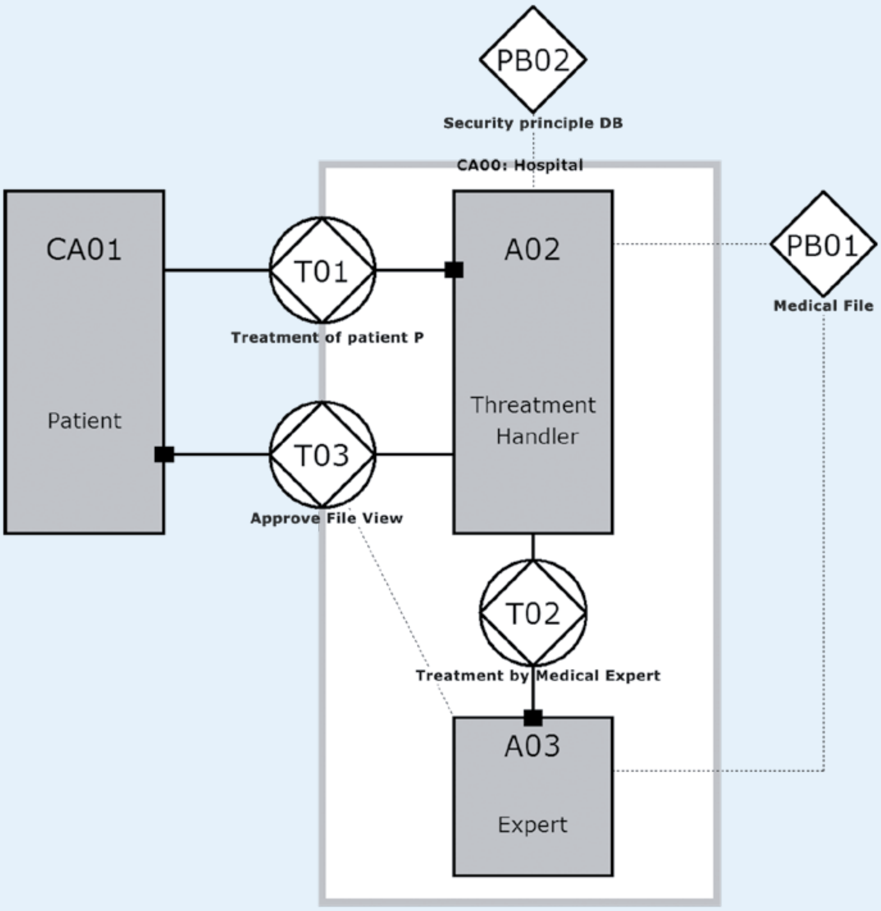


Figure 3: ATD with Production Bank 'Medical File'

Namely the I-layer and D-layer. When we go down into this I-layer of the organization and model the so called I-organization we explore all information transactions and informational actors[4]. Based upon these I-transactions we determine what CIA breaches these transactions reveal. It is here where the necessary principle scenarios need to be designed in order to take adequate measures to avoid negative impact. This is typically an exercise done by people with technical skills. After defining these principles the information (security) manager together with his business responsible people has to decide which principle to implement (and how much budget to allocate).

SDEMO Checklist

To align business and ICT people and fully benefit from the power by separation of B-I-D transaction layers of DEMO a checklist is developed. Business as well as technical people can use this checklist per layer of the organization and per transaction. This SDEMO checklist should have a dynamic character and is filled with the basic CIA security related questions that might arise during transaction

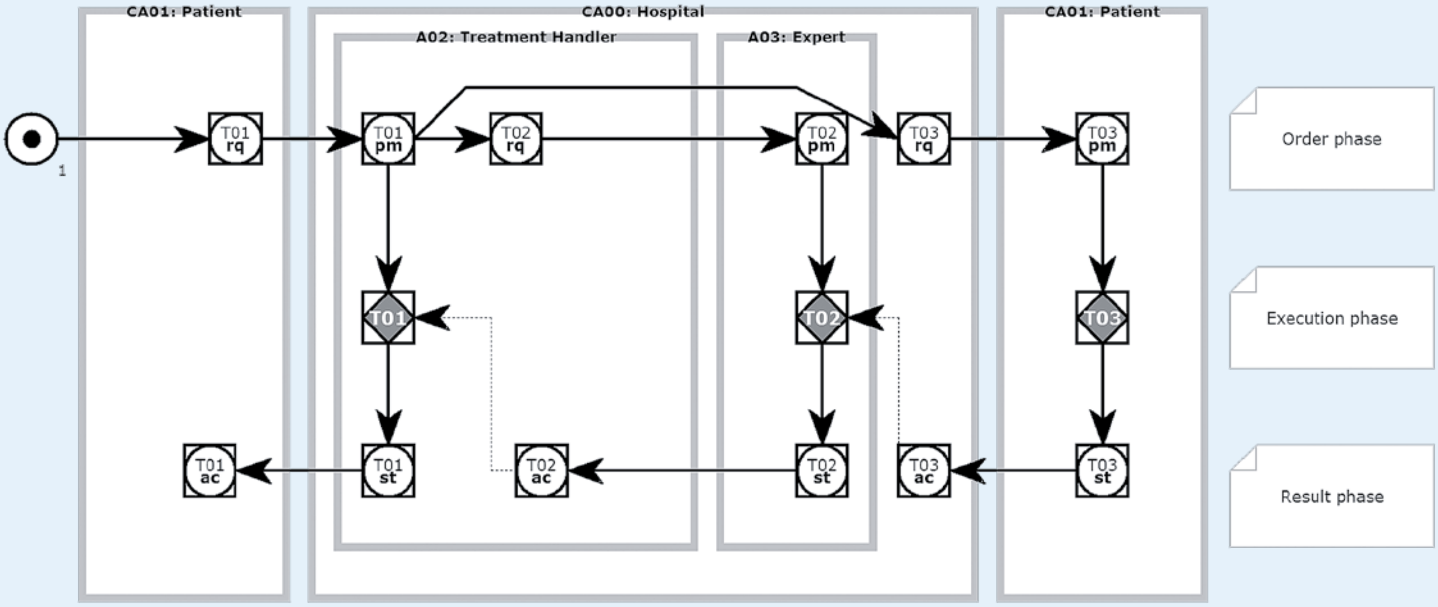


Figure 4: The DEMO process Structure Diagram displaying the state of a transaction

[4] *The specification of the I-layer according to DEMO with security principles is provided in the appendix*

Demo layer	SDEMO Question
Performa (business)	1. Is this transaction business critical? 2. What if this transaction fails? 3. What if this transaction is not able to order, execute or request? 4. If transaction completed, what (information) result do I get and what's the criticality of this fact?
Informa (information)	1. Do I know all information actors involved in the transaction? 2. How are identification, authentication, authorization and administration handled? 3. What is the result, the impact on the business if information (during process) is stolen, manipulated or lost? 4. Is there an information handling procedure in place?
Forma (data)	1. Where is the data stored? Physical/virtual? 2. How can data be accessed? 3. Is there an access control policy and are control methods in place? 4. How is backup and restore handled?

handling.
We use the DEMO notation to effectively display all actors and transactions at an ontological level. After that we use the SDEMO checklist to address security issues that might arise. By using the combination of methods this method addresses (to stakeholders) the criticality of protecting the enterprise critical assets by interaction in a complex environment (extended enterprise). Most of the used DEMO basic modeling techniques like the construction model, process model, state model and action model have good starting points to extend the design with security principles. Either you use the CIA principles or you use standard baselines like BS, Cobit, ISO/IEC, HIPAA, NEN, SOx or other compliancy regulators, depending on the contextual influences (corporate governance) that effect the enterprise in question.

Rapidly changing technologies highly affect today's architecture principles. For example: implementation of security practice frameworks like ISO/BS or corporate governance guidelines like SOx might lead to separation of data and information flows in highly secure environments (financial data) on a physical level. For example, even though the introduction of virtualization already made his entrance in the enterprises construction level, the principles for network, server, storage virtualization of the data layer is embryonic. Therefore the D-layer needs further research as well as the transformation when information becomes data and vice versa.

Conclusion

Rapidly changing technologies serving the business require a swift way of re-modeling enterprises and their architectural principles. DEMO is a powerful methodology to design the essential layers by using different models. Implementing security principles into these models is limited due to the fact that I limited my research only to the business layer and the information layer. In practice I discovered that it is necessary to involve business people into principles implementation. Not only because they need to be aware of the business impact if they don't, but also because of the financial effects. The SDEMO checklist helps business people understand the possible security breaches and their impact on business transactions. More in-depth: overlaying the several business oriented models within DEMO with the security principles of Confidentiality, Integrity and Availability will result in an effective theoretical way of modeling. This can be done by using the Process Structure Diagram (PSD) combined with the information requirements diagram. This will not enlighten the necessary measures we need to take to avoid a security breach. This can be done by making use of the I-organization design together with the detailed transaction description. In this description we determine which CIA breach we might be facing. After the detailed description of these breaches and the possible principle scenarios stakeholders can make well argumented security principle decisions (investments). I found out that DEMO in itself was limited here by not involving the context in these decisions. Mainly because we are talking about extended enterprises I have searched for other techniques to add to DEMO and accomplish a fully integrated modeling technique. I therefore added the Extended Enterprise Framework of Dr. Martin Op 't Land to DEMO and initiated an ICT and business alignment security modeling technique. In my opinion it needs more research and practice on the data layer of the enterprise and also a better practice of distinguishing security process techniques (like ISO, ITIL) and security technology techniques (like segmentation, encryption, signing).

Also further research is needed to further sharpen the SDEMO questions and checklist. The objective should be to make sure checklist are formulated simple and brief in order to cover all possible breaches per layer. Further research also needs to be done to introduce checklists based upon compliancy guidelines or best practices. For example the practical implementation of SDEMO in combination with best practices (ISO/IEC27001) or practical implementations (ISO/IEC27002).

Literature

- Enterprise Ontology by Prof. Dr. Ir. J.L.G. Dietz. ISBN nr. 3-540-29169-5
- Rapid Enterprise Deployment by Prof. Dr. Ing. J.B.F. Mulder MBA , MSc.
- Applying architecture and Ontology to the splitting and allying of Enterprises by Dr. Drs. M. Op 't Land. ISBN nr. 978-90-71382-32-1.
- Informatiebeveiliging onder controle door Dr. Ir. P. Overbeek e.a. RE. ISBN nr. 90-430-0692-0 .
- Implementing Information Security based upon ISO27001/ISO17799 by management guide. ISBN 978-90-77212-783.

More info

- Official DEMO website: www.demo.nl
- Full research paper on: www.b-able.nl