Security and integrity requirement in socio-technical systems

Mohamad Gharib

UNIVERSITY OF TRENTO - Italy
Information Engineering
and Computer Science Department

Outline

1. Background
2. Problem
3. Information integrity (attributes)
4. Security/Integrity models
5. Integrity requirements
6. Case study
7. Requirements Eliciting Process

1. Background

- Organizations depend on information to perform their everyday tasks, the performance of these tasks are highly related to the information reliability.
- Nowadays, most of the organizations intend to secure their information systems. However, designing a secure information system is not an easy task.
- It has long been recognized that integrity, together with confidentiality and availability, is a fundamental requirement for secure information systems.

2. Problem

- Considering the integrity requirements is hard due to the nature of these systems mainly because of two reasons:
  1. information is created, stored and exchanged between autonomous systems. It can exist in different forms, it can be communicated or transferred in different means.
  2. people are considered as an integrated part of these systems, and they can be a main source for compromising the integrity of the data especially when they create, modify, share, exchange or transfer the data. However, this problem is mainly because of the following two reasons:
     - Information creation, modification, sharing, exchanging or transferring do not take place in an ideal environment all the times;
     - In some cases, the information creation, modification, sharing, exchanging or transferring is not fully under the control of the IT system, since not all the people's actions are automated.

3. information integrity

- Integrity definition changes based on the domain in which it has been defined.

	Accuracy	Completeness	Consistency	Existence	validity	Reliability	Availability	Timelines
Cobit [18	X	X	X	X				
Bovee [8]	X	X		X	X			
Boritz [7]	X		X		X			X
Mandke [24]	X		X		X	X		
Hansen [16]	X						X	X

- Information integrity is concerned with preserving the meaning of information, with preserving the completeness and consistency of its representations within the system, and with its correspondence to its representations external to the system [24].

4. Security/Integrity models

1. Bell-LaPadula Model (1973).
2. Biba Model (1977).
3. Lipner Commercial Integrity Model (1982).
4. GOGUEN AND MESEGUER MODEL (1982).
5. CLARK AND WILSON MODEL (1987).

4.1 Biba Model

- Biba model supports the access control of both subjects and objects. Each subject and object have an integrity level associated with it. Each integrity level will be represented as L = (C, S)

- The Biba model elements support five different integrity policies: (1) Low-Water Mark Policy, (2) Low-Water Mark Policy for Objects, (3) Low-Water Mark Integrity Audit Policy, (4) Ring Policy, and (5) Strict Integrity Policy.

- **Strict Integrity Policy:**
  - Simple Integrity Condition: $s \in S$ can observe $o \in O$ if and only if $i(s) \leq i(o)$ ("no read-down").
  - Integrity Star Property: $s \in S$ can modify $o \in O$ if and only if $i(o) \leq i(s)$ ("no write-up").

- **Low-Watermark Policy:**
  - Integrity Star Property: $s \in S$ can modify $o \in O$ if and only if $i(o) \leq i(s)$ ("no write-up").
  - A subject may examine any object. If $s \in S$ examines $o \in O$ then $i'(s) = \min(i(s),i(o))$, where $i'(s)$ is the subjects integrity level after the read.

4.2 CLARK AND WILSON MODEL.

- There are two keys to the Clark and Wilson integrity policy:

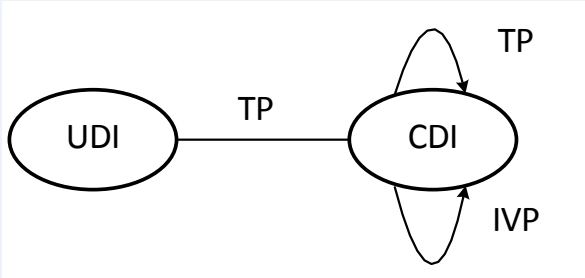
  1-The well-formed transaction: user cannot manipulate data arbitrarily, but only in constrained ways that preserve or ensure the internal consistency of the data.

and

  2- separation of duty: to ensure the external consistency of data objects.

- The Clark and Wilson model is defined in terms of four elements:

  1-constrained data items (CDIs),
  2-unconstrained data items (UDIs),
  3- integrity verification procedures (IVPs),
  4- transformation procedures (TPs).



4.3 Integrity in RE

- Abuse cases [17] and misuse case [18] both did not provide a special primitives for modeling and reasoning about integrity, even they both provide high level modeling and reasoning mechanisms to capture threads to the system.

- SecureUML [3] was mainly developed to model access control policies. In UMLsec [13], integrity was modeled as a constraint, which can restrict unwanted modification, but data still can be modified in several other ways.

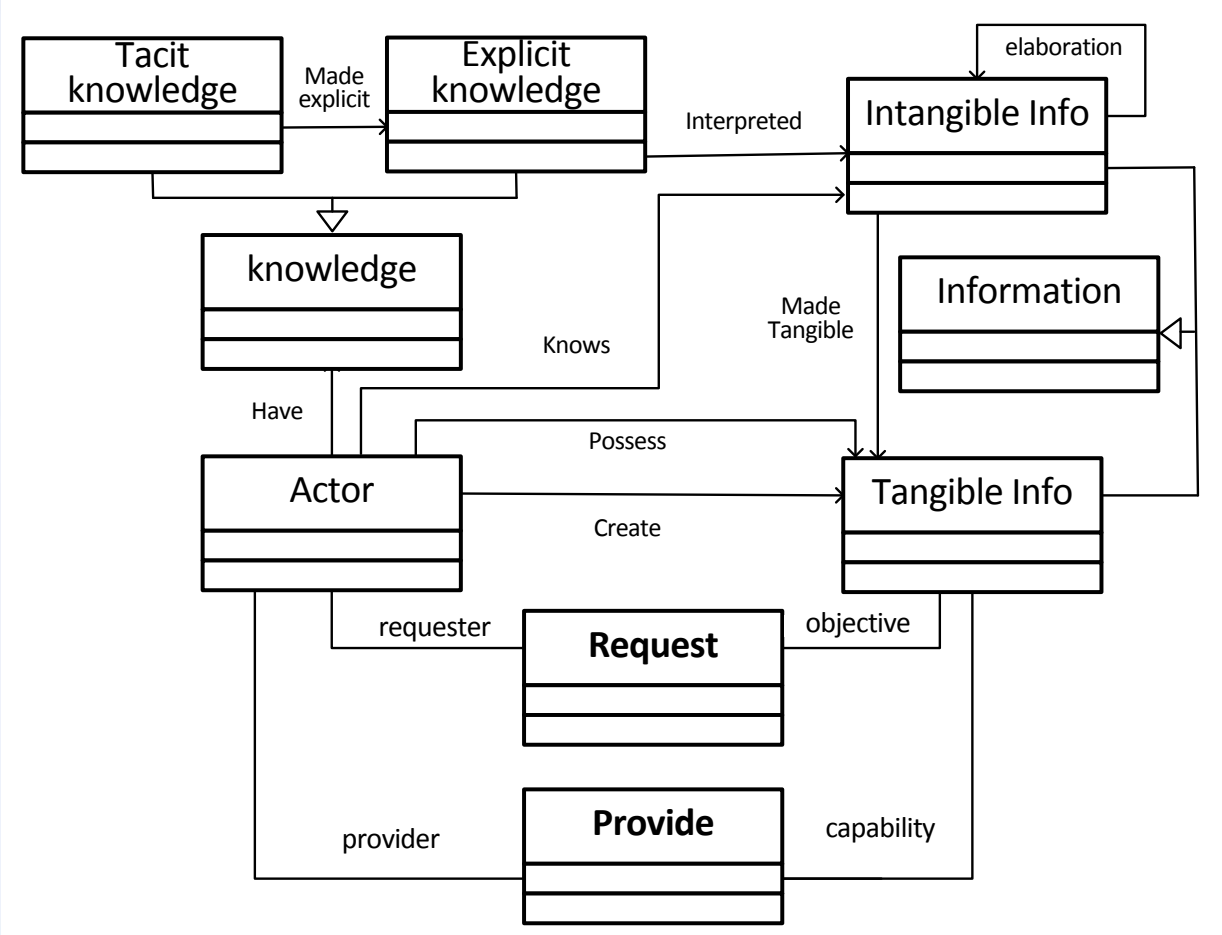
- Abuse frame [14] like UMLsec addresses the integrity problem (modification) by preventing unauthorized actors from modifying the data or prevent authorized actors from doing unauthorized modifications.

5. Integrity requirements

- To address the integrity requirements of the system ,we have to address the following four points:
- 1. Prevention and detection of errors,
- 2. Control of information-flow,
- 3. Data verification,
- 4. Data validation.

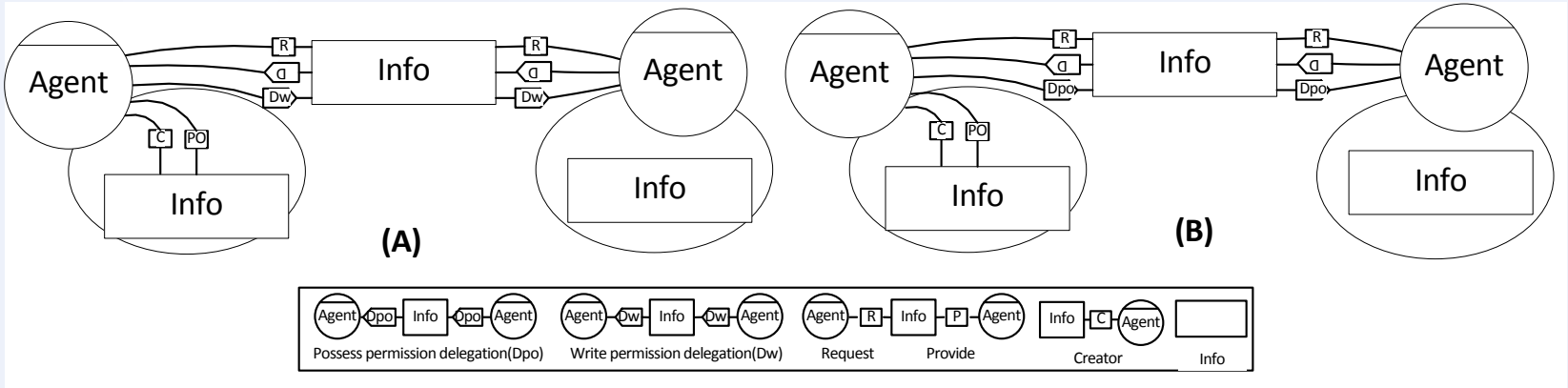
5.1 Prevention and detection of errors

1. Information sources.
2. Information creations, possess and provide.



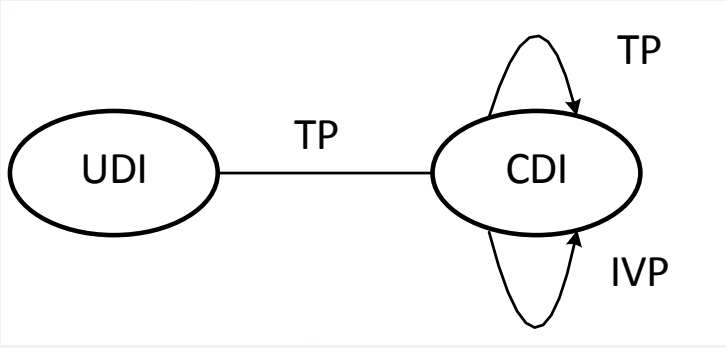
5.2 Control of information-flow

1. Integrity models concerning with the notion of information-flow include the *Strict Integrity* model and the *Low Water-Mark* model.
2. The level of information integrity will be changed during its flow based on the permissions that the actors have.



5.3 Data verification

1. Data verification requirement states that all data items must be verified (accurate and complete).
2. The requirement states that as long as the well-formed procedures receive verified data, the transaction takes data from one valid state to another.



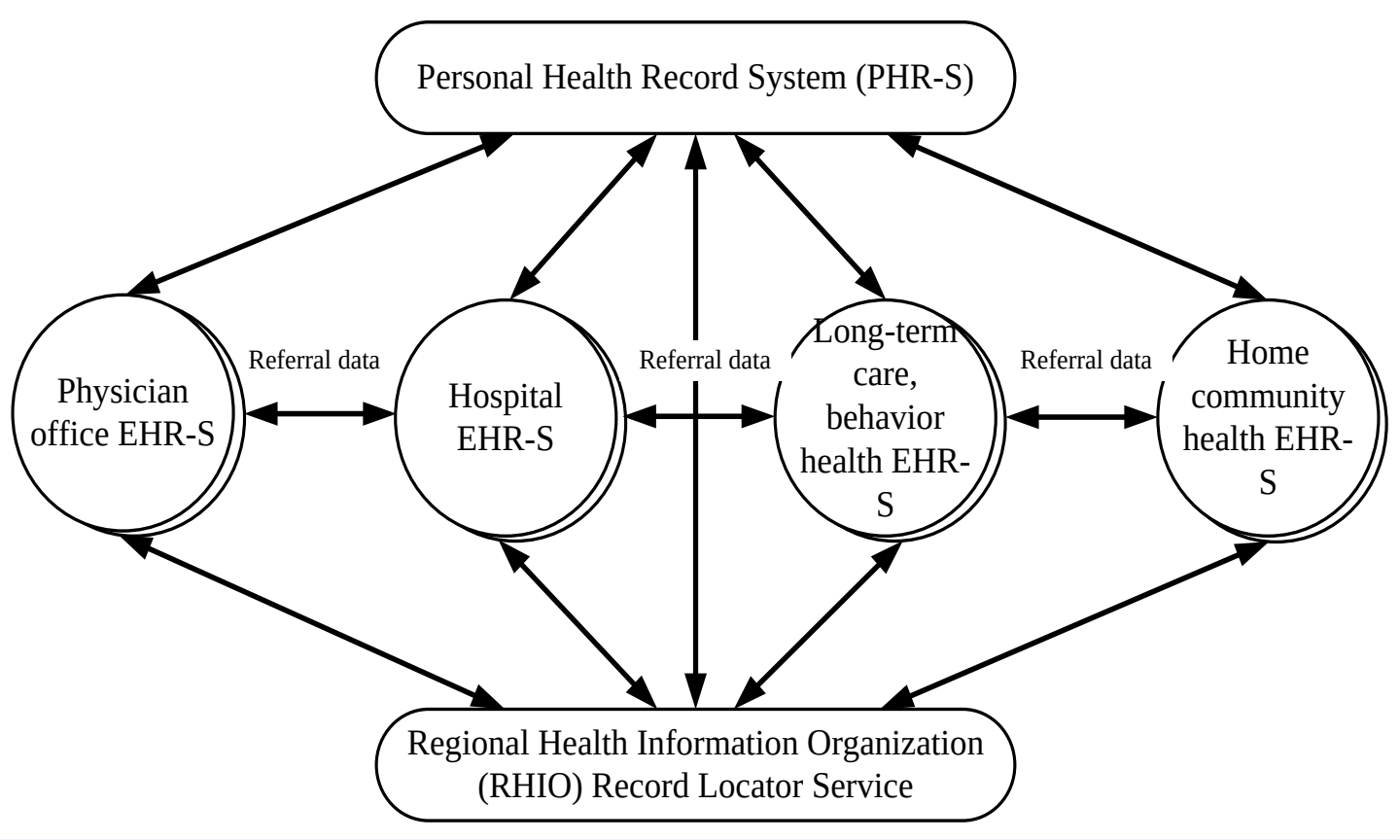
5.4 Data validation.

1. Certain data item may lose its integrity based on factors such as time, event etc.
2. Data validation process should look for inconsistency in the data items and report the same. It helps to maintain consistency between internal and external world.

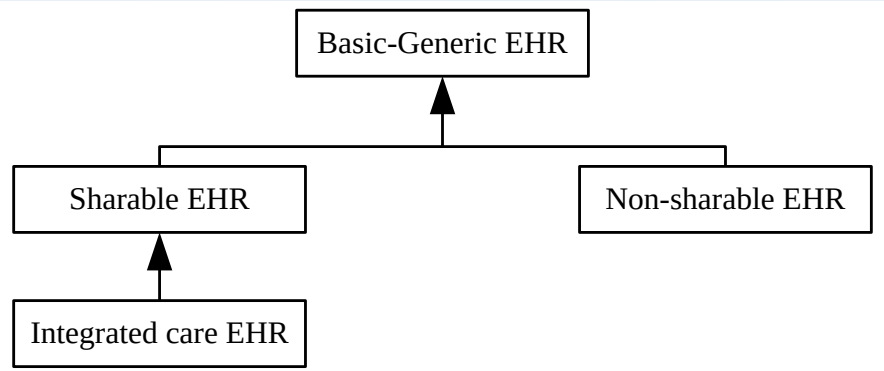
6.1 Case study – domain analysis

- A healthcare system is an organization of people, institutions (clinics, hospitals, laps …) and resources to deliver healthcare services to meet health needs of target population.
- A variety of health information systems; these systems create, exchange and share medical records or electronic health records (EHR).
- Due to the complex nature of these systems, they may not be able to preserve the integrity of the shared and exchanged information.

6.1 Case study – domain analysis



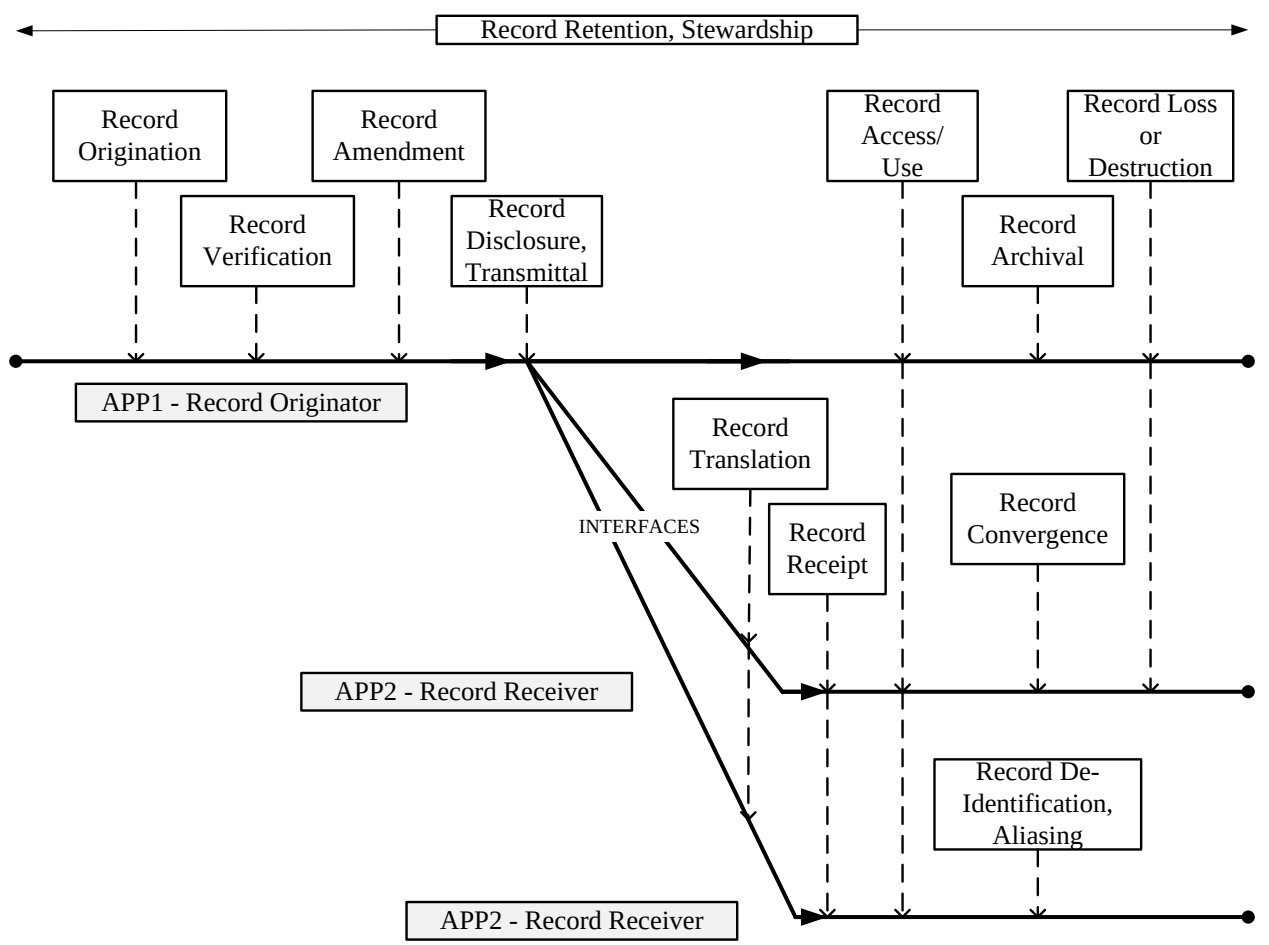
6.2 EHR types



1. **The basic–generic EHR** is a repository of information regarding the health status of a subject of care, in computer processable form.
2. **The non-shareable HER,**
3. **The shareable HER,**
4. **The Integrated Care EHR (ICEHR)** Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information which is retrospective, concurrent, and prospective.

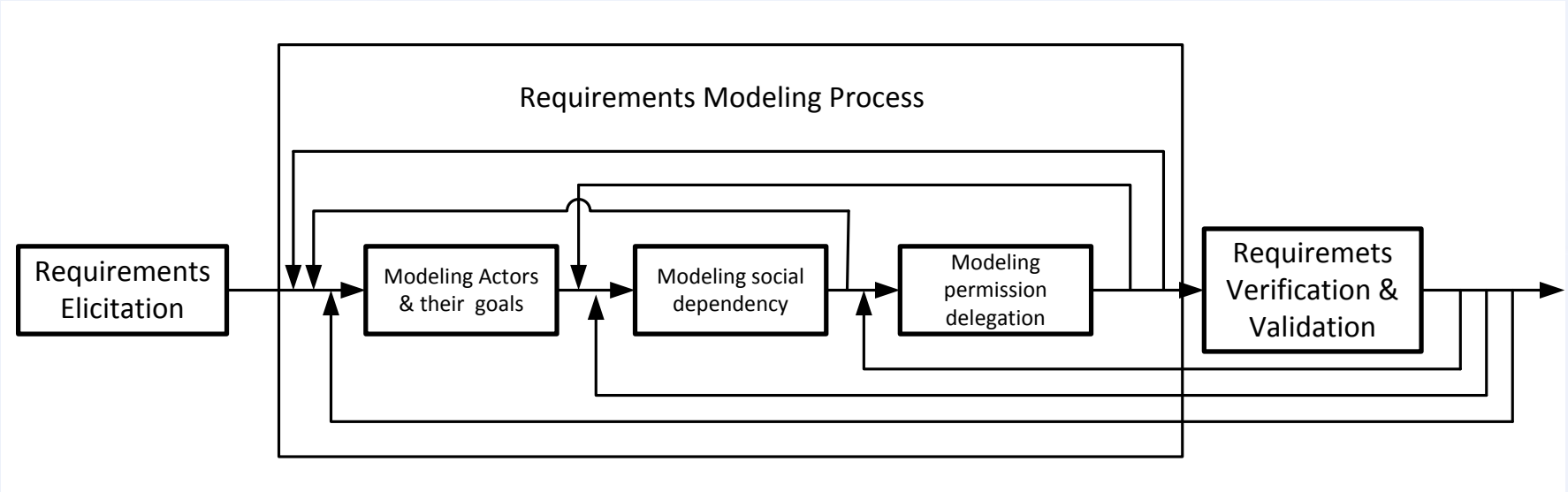
ISO/TS 18308:2004, ISO/TR 20514:2005.

6.3 EHR life cycle



1. Figure From ISO 21089, “Health Informatics – Trusted End-to-End Information Flows”

7. Requirements Eliciting Process



References

[1]Ali, R, et al (2010) A goal-based framework for contextual requirements modeling and analysis RE.

[2] Baldauf .M et al (2007) A survey on context-aware systems.IJAHUC2(4).

[3] Bresciani, P et al (2004) Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*.

[4] Cuppens, F., and Saurel, C. (1996) Specifying a Security Policy: A Case Study. IEEE Computer Society Computer Security Foundations Workshop CSFW9.

[5] Dey, A.K. and Abowd, G.D. (2000) Towards a better understanding of context and context-awareness, ACM Press, New York, 2000.

[6] E. E. Community. Information Technology Security Evaluation Criteria (ITSEC). Technical report, 1990. http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

[7] Emery , et al (1960) L. Socio-technical systems. In Management sciences: Models and techniques, vol. 2. Pergamon Press.

[8] Finkelstein, A. and Savigni, A. (2001) A framework for requirements engineering for context aware services, (*STRAW 01)*.

[9] Ferraiolo, D.; Cugini, J. & Kuhn, D. Role-based access control (1995): Features and motivations Proceedings of 11th Annual Computer Security Application Conference.

[10] Gelfond, M. & Lifschitz (1991), V. Classical negation in logic programs and disjunctive databases New generation computing, Springer.

[11] Hartmann, H. and Trew, T. (2008) Using feature diagrams with context variability to model multiple product lines for software supply chains, *(SPLC 08)*.

[12] Henderson-Sellers, B. & Giorgini, P. Agent-oriented methodologies IGI Global, 2005.

[13] ISO/IEC. Code of practice for information security management. ISO/IEC 17799:2005, 2005.

[14] ISO/IEC. Code of practice for information security management. ISO/IEC 27002:2007, 2007.

References

[16] Kang, K.C., et al (1990), Feature-oriented domain analysis (foda) feasibility study. Technical Report.

[17] Kang, K.C., et al (1998), Form: A feature-oriented reuse method with domain; specific reference architectures. Annals of Software Engineering.

[18] Lamsweerde, A.V. (2001) Goal-Oriented Requirements Engineering: A Guided Tour. In Proc. of the 5th IEEE (RE).

[19] Lapouchnian, A. and Mylopoulos, J. (2009), Modeling domain variability in requirements engineering with contexts (ER).

[20] Lee, J. and Muthig. D. (2008), Feature-oriented analysis and specication of dynamic product reconguration. In ICSR.

[21] Liaskos,S., et al (2006), On goal-based variability acquisition and analysis. *Proc. 14th IEEE.*

[22] Lin. L, et al (2003),. Introducing abuse frames for analysing security requirements IEEE Computer Society.

[23] Liu, L.; Yu, E. & Mylopoulos, J. (2003) Security and privacy requirements analysis within a social setting Proc. of RE, Citeseer.

[24] Massacci, F ., et al (2007), N. An ontology for secure socio-technical systems Handbook of Ontologies for Business Interaction. The IDEA Group, Citeseer.

[25] Mccarthy, J. (1993), Notes on formalizing contexts. *Conference on Artificial Intelligence.*

[26] McDermott, J. & Fox, C. (1999) Using abuse case models for security requirements,(ACSAC'99).

[27] Mouratidis, H., et al (2003), Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems. Proc. CAiSE.

[28] Osborn, S.; Sandhu, R. & Munawer, Q.(2000) Configuring role-based access control to enforce mandatory and discretionary access control policies ACM Transactions on Information and System Security.

[29] Pohl, K., et al (2005), *Software Product Line Engineering: Foundations, Principles, and Techniques*. Springer.

[30] Salifu, M, et al (2007), Using problem descriptions to represent variability for context-aware applications. *First International Workshop on Variability Modelling of Software-intensive Systems*.

[31] Schilit, B. N et al (1994). Context-aware computing applications. In *IEEE Workshop.*

References

[32] Siena, A., et al (2009). Designing law-compliant software requirements. In (ER'09).

[33] Sindre, G. & Opdahl, (2000), A. Eliciting security requirements by misuse cases Technology of Object-Oriented Languages and Systems.

[34] Strang, T. and Linnhoff-Popien, C. (2004), A Context Modeling Survey, UbiComp.

[35] Wang, X. H., et al (2004). Ontology based context modeling and reasoning using owl. In *PERCOMW '04.*

[36] Yu, E. and Mylopoulos, J. (1998), Why goal-oriented requirements engineering, RE.

[37] Coutaz, J. (2009), Context is key Communications of the ACM, ACM, 2005, 48, 49-53.

[38] Schmidt, A., et al (1998), There is more to Context than Location. Computers and Graphics.

[39] Yu, Y.; et al (2008), Configuring features with stakeholder goals, ACM.

[40] Yu, E. (1995),Modelling strategic relationships for process reengineering. Ph.D. Thesis.

[41] Van Lamsweerde, A. , et al (2003), From system goals to intruder anti-goals: attack generation and resolution for security requirements engineering Requirements Engineering for High Assurance Systems (RHAS'03).

[42] Van Lamsweerde, A. & Letier, E.(2000) Handling obstacles in goal-oriented requirements engineering Software Engineering, IEEE Transactions on.

[43] Zannone, N. (2007), A Requirements Engineering Methodology for Trust, Security and Privacy. . PhD thesis, University of Trento,.

[44] Zhang, G. & Parashar, M. (2003),Dynamic context-aware access control for grid applications Grid Computing, 2003. Proceedings. Fourth International Workshop on.

[45] Zave, P. Classification of research efforts in requirements engineering ACM Computing Surveys (CSUR), ACM, 1997, 29, 315-321.


Thank you