SECURITY REQUIREMENTS ENGINEERING

The MIT Press Information Systems Series

Michael Papazoglou, Eric Yu, Florian Matthes

Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering
Nikola K. Kasabov, 1996

Advances in Object-Oriented Data Modeling
Michael P. Papazoglou, Stefano Spaccapietra, and Zahir Tari, editors, 2000

Workflow Management: Models, Methods, and Systems
Wil van der Aalst and Kees Max van Hee, 2002

A Semantic Web Primer
Grigoris Antoniou and Frank van Harmelen, 2004

Aligning Modern Business Processes and Legacy Systems: A Component-Based Perspective
Willem-Jan van den Heuvel, 2006

A Semantic Web Primer, Second Edition
Grigoris Antoniou and Frank van Harmelen, 2008

Service-Oriented Computing
Dimitrios Georgakopoulos and Michael P. Papazoglou, editors, 2008

At Your Service: Service-Oriented Computing from an EU Perspective
Elisabetta di Nitto, Anne-Marie Sassen, Paolo Traverso, and Arian Zwegers, editors, 2009

Meta-Modeling for Method Engineering
Manfred A. Jeusfeld, Matthias Jarke, and John Mylopoulos, editors, 2009

Social Modeling for Requirements Engineering
Eric Yu, Paolo Giorgini, Neil Maiden, and John Mylopoulos, editors, 2011

Modeling Business Processes: A Petri Net-Oriented Approach
Wil van der Aalst and Christian Stahl, 2011

A Semantic Web Primer, Third Edition
Grigoris Antoniou, Paul Groth, Frank van Harmelen and Rinke Hoekstra, 2012

Security Requirements Engineering: Designing Secure Socio-Technical Systems
Fabiano Dalpiaz, Elda Paja, and Paolo Giorgini, 2016

SECURITY REQUIREMENTS ENGINEERING

Designing Secure Socio-Technical Systems
Public Solutions (Review Questions)

Fabiano Dalpiaz
Elda Paja
Paolo Giorgini

The MIT Press
Cambridge, Massachusetts
London, England

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data is available.

ISBN ISBN: 978-0-262-03421-0

10 9 8 7 6 5 4 3 2 1

Solutions to the Exercises (Chapter 2)

Review questions

Q2.1. *Explain what information assets are, and provide some examples in the context of a bank.*
Information assets are information that organizations depend on to function properly. An information asset has value to the organization and requires protection. Some examples for a bank are the information of bank accounts owners, the balance of each account, the customers' credit rating, mortgage application data, the reason for approving or rejecting a mortgage application, the code to unlock the safebox, and so on.

Q2.2. *What is the difference between confidentiality and privacy?*
Confidentiality is a broader notion that encloses privacy. Confidentiality is concerned with ensuring that private or confidential information is not made available to unauthorized users and that (*privacy*) the users can control or influence what information related to them may be used and for what purposes. Information (for example, a citizen's birthdate) can be kept private—by employing access control policies—even without allowing the information owner (the citizen) to control its use.

Q2.3. *Consider the security aspect of authenticity. Explain the difference between user authentication and data authentication. What are the mechanisms to ensure authenticity?*
Authenticity is the property of being genuine and being able to be verified and trusted. *User authentication* is about providing adequate credentials to convince another party that a user is really who he claims to be. For example, a student could authenticate himself by showing his identity card. *Data authentication* is concerned with the genuinity of stored data. For example, ensuring that the student grades stored in the university information system are genuine, verifiable, and trustworthy.

Q2.4. *What is accountability? Why is it an important security notion?*
Accountability is about correctly tracing the actions that an entity has performed. This is essential for communication between actors, for full accountability would make it impossible to claim that a message was not sent or received, and to pretend that a message was sent by someone else.

Q2.5. *How do threats and vulnerabilities relate with each other?*
Both threat and vulnerability are essential notions for risk analysis. A threat is a potential cause of an incident, which may harm systems or

organization. An example of threat is the disclosure of confidential data or its non-authorized modification. On the other hand, a vulnerability is an exploitable weakness in either an information system, security procedures, internal controls, or implementation. An example of vulnerability is a bug in the database's access control system, which enables external attackers to read and modify the data in the database.

Q2.6. *Define the notion of risk, and explain how to derive this value.*
The concept of risk (or risk value) measures the quantified impact of a threat being realized (via the exploitation of a vulnerability). As such, risk is computed through a function that combines the effects of the event and the likelihood of occurrence. Qualitative risk analysis and assessment (that is, low-medium-high values) propose to use a risk matrix that combines qualitative values for the threat-asset impact with the qualitative likelihood of a vulnerability to occur.

Q2.7. *What is public key encryption? How does it differ from private key encryption?*
Public key encryption is a family of encryption techniques that rely on the property of asymmetry. Unlike private key encryption, sender and receiver do not share the same key. Every person possesses a private key and keeps it secret, and a public key that he shares publicly. These keys are complementary: a message that is encoded with the private key can be decrypted with the public key, and vice versa. To exchange a message via public key encryption, the message is first ciphered using the receiver's public key, the encrypted message is transmitted, and the received message is deciphered using the receiver's private key. This ensures that the receiver be the only able to decrypt the message.

Q2.8. *What are the key elements of access control? What security aspects does access control contribute to?*
Access control supports confidentiality as well as integrity of data. Its main elements are the *access actions* that are being regulated; the *subject*, that is, the entity whose actions are constrained; and the *object*, that is, the passive entity on which the subject can(not) perform certain actions.

Solutions to the Exercises (Chapter 3)

Review questions

Q3.1. *What is a socio-technical system? How does it differ from other types of systems? List a few examples.*
A socio-technical system is a composite system that is defined by the interactions among humans, organizations, and software systems. These actors interact to fulfill their own goals and requirements. Unlike software systems and social systems, socio-technical systems emphasize the interdependencies between social and technical systems, which calls for a holistic approach when it comes to their design. Examples of socio-technical systems are smart cities, educational and healthcare systems, and any modern IT-enabled organization.

Q3.2. *What is the difference between a role and an agent?*
A role is an abstract characterization of an actor that entails certain responsibilities for the concrete actors (agents) playing that role. For example, the role of physician includes responsibilities such as visiting sick patients that reside in the neighborhood, prescribing medicines and further examinations, and so forth.

Q3.3. *Define assets. What is the difference between informational and intentional assets?*
An asset is anything that holds value to an organization or to an individual. In STS-ml, information assets are information that actors care about, such as demographic data, e-mails, and certificates. Intentional assets refer to the intentions (goals) of actors; those are assets because the actors care for their fulfillment. Examples of intentional assets are the goals blood donated, assignment graded, and blood analyzed.

Q3.4. *How are threats represented in STS-ml?*
Threats are represented via two primitives: the event element and the threatens relationship. A threat is denoted by linking an event to a goal or a document via a threatens relationships. The semantics of this linkage is that the occurrence of the event poses a threat that may compromise the goal or the document (its availability, integrity, and so on).

Q3.5. *List the main differences between information and document.*
Documents represent concrete and transferable entities that actors may exchange, such as a certificate, an identity document, and a driving license. Information are the primary assets that the actors care about,

such as the birthdate that is represented in (made tangible by) an identity document, a patient's medical status, and the grade obtained in a certain exam.

Q3.6. *Explain the part-of relationship, also detailing which elements it can relate in STS-ml.*
The part-of relationship structures information and documents into subelements. The relationship applies to homogeneous elements: it can link two documents, or two information entities. The meaning is that one entity E_1 is essential part of another entity E_2.

Q3.7. *Describe the security requirements types that STS-ml supports.*
STS-ml supports different types of security requirements, which belong in the following major classes:

- Confidentiality ensures that private or confidential information be not made available to unauthorized users. Confidentiality requirements are expressed through authorizations.
- Integrity requirements ensure that information be not changed or destroyed in an unauthorized way, and is supported through authorizations where modification is prohibited.
- Availability, ensuring that the system works promptly. STS-ml supports constraining the availability level of goals and documents.
- Authenticity concerns the property of being genuine and being able to be verified and trusted. In STS-ml, this is supported by constraining goal delegations and document transmissions.
- Reliability addresses the consequences of accidental errors, including non-designed uses. STS-ml supports reliability by imposing requirements on trustworthiness and redundancy.
- Accountability is concerned with the requirements for the actions of an entity to be traced uniquely to that entity. STS-ml supports this requirement type via non-repudiation constraints, separation of duties, and combination of duties.

Q3.8. *Explain the difference between delegator and sender authentication.*
The requirement of authenticity requests that an actor involved in a

goal delegation or a document transmission be authenticated. Specifically, delegator authentication applies to the actor from which a delegation originates, while sender authentication applies to the actor that transmits a document.

Solutions to the Exercises (Chapter 4)

Review questions

Q4.1. *In which view is the information flow captured in STS-ml? Through which primitives?*
It is captured in the social view through the primitive of document transmission. This is an indirect representation that is fully understood by combining the social view with the information view. The information view details the information that the documents make tangible; thus, one understands the information flow by examining the transmitted documents in terms of the information they consist of.

Q4.2. *What is the difference between the social view and the authorization view?*
The social view focuses on the social and organizational aspects: the actors are represented along with their objectives and interactions with others. The authorization view models the permissions and prohibitions among the actors in the socio-technical system. These two views focus on different yet complementary aspects of socio-technical systems modeling: the actual flow of documents and goal delegations among actors (social view), and the security requirements expressed through authorizations (information view).

Q4.3. *How does the social view differ from the information view?*
The social view represents actors, their objectives, and their interactions. The information view analyzes a specific aspect, that is, the information that the documents contain, and how documents and information are structured. As explained in the solution to Q4.1, one can combine the two views to determine what information is being exchanged through the transmission of documents.

Q4.4. *In which view(s) are stakeholders' assets represented in STS-ml?*
Mostly in the social view and the information view. The social view represents the primary intentional asset type—goals, the secondary

intentional assets—subgoals, and the secondary information assets—sdocuments. The information view represents both the primary and secondary information assets: information and documents. The authorization view refers to these assets (authorizations are granted on information and can be limited to the scope of specific goals).

Q4.5. *In which view(s) are threats represented in STS-ml?*
They are represented in the social view through the modeling of an event that threatens a goal or a document.

Q4.6. *In which view(s) are security requirements captured in STS-ml?*
They are captured in the social view and in the authorization view. The social view expresses a number of requirements as constraints over goal delegations and document transmissions, as well as accountability requirements such as separation and combination of duties (both for roles and goals). The authorization view enables the implicit specification of security requirements through the permissions and prohibitions that the authorizations entail.

Q4.7. *Explain what implicitly expressed security requirements are and how they differ from explicitly expressed ones.*
Implicitly expressed security requirements are modeled as authorizations wherein certain operations (read, modify, produce) are prohibited, when the scope is limited to a specific set of goals, and when reauthorization is not allowed. They differ from explicitly expressed requirements in that they are derived from the drawn authorizations, instead of being expressed through a specific primitive (the constraints on delegations and transmissions, as well as separation and combination of duties).

Q4.8. *What are the main reasons for having more than one view in a modeling language?*
The principal reason is to cope with the complexity of the models by separating different concerns into complementary views. These views are tightly intertwined; thus, some concepts are visible in multiple views.

Solutions to the Exercises (Chapter 5)

Review questions

Q5.1. *When is an STS-ml model well formed?*
An STS-ml model is well formed when it adheres to the syntactic rules of the language. For example, a model is not well formed when a goal is decomposed to only one subgoal, or when a delegation cycle exists.

Q5.2. *Why is it important to verify well-formedness?*
The major reason is to avoid those ambiguities that would arise in security reasoning with an ill-formed model. A syntactically correct model is prerequisite to executing more sophisticated reasoning.

Q5.3. *What is covered in security analysis? Discuss the categories, identifying their differences.*
Security analysis covers a number of reasoning techniques that enable determining conflicts between (security) requirements. For STS-ml models, two main categories of conflicts exits:

- Conflicts between security requirements: two or more requirements cannot be fulfilled by the same socio-technical system. For example, two conflicting authorizations where one actor is granted both permission and prohibition for the same information by two other actors.
- Conflicts between actors' business policies and security requirements. For example, an actor's business policy may involve transferring some document to a third party, and that actor was required by the information owner to avoid transferring any documents that contain the considered information.

Q5.4. *How is the impact of threats calculated over STS-ml models?*
This analysis technique propagates the effect of an event over goal trees and goal/document relationships within actor models (the reads, modifies, and produces relationships), as well as delegations and document transmissions. The reasoning starts from the specified threatening events, and marks as threatened all the elements that can be reached through the following rules:

- The goal/document linked to the event through a threatens link is threatened;
- If a subgoal is threatened, the parent goal is threatened too;

- If a threatened goal is delegated, the copy of the goal within the delegator's actor model is threatened too;
- If a threatened goal produces a document, the document is threatened too;
- If a threatened document is used/modified by some goal, the goal is threatened too;
- If a threatened document is transferred from another actor, the sender's document is threatened too;
- If a threatened document consists of other documents, its subdocuments are threatened too.

Q5.5. *Why are automated reasoning techniques useful in the process of creating STS-ml models?*
STS-ml uses a rich ontology a concepts which enable constructing expressive models. Along with the use of three complementary views, this makes it possible for the models to be inconsistent. Moreover, since security requirements are expressed by the various stakeholders in the sociotechnical system, conflicts may inherently exists. Automated reasoning is useful for the security requirements engineer to identify conflicts as soon as possible so that a compensation can be identified.

Q5.6. *Provide three examples of authorization conflicts in the context of mobile banking.*

- The bank permits the mobile app developer to read documents representing the personal data of the customer, while the customer prohibits the bank from transferring rights about his personal data;
- The customer authorizes the mobile app developer to produce documents representing the bank account balance, while the bank prohibits that;
- The mobile app developer prohibits the bank from distributing the encryption algorithm, while the customer permits the bank to do so, because he has followed an information security course that taught him the importance of employing open security algorithms.

Q5.7. *Explain the notion of a conflict between business policies and security requirements. Provide one example.*

This type of conflict arises when the way of achieving goals in the social view conflicts with the security requirements expressed on delegations and transmissions, and through authorizations. An example of conflict is when an actor is delegated a goal with a non-redelegation security requirement and the actor's business policy involves redelegating (part of) the goal.

Solutions to the Exercises (Chapter 6)

Review questions

Q6.1. *What steps are prescriptive in the STS method process?*
The steps in the STS process are not prescriptive; they are a guideline for the use of the STS method, but the analyst may choose to customize the process and to perform the activities following a different order. It is, however, essential that the three views are completed, and that they are checked both for consistency and for the absence of security conflicts.

Q6.2. *Can the specification phase be executed before analysis activities are executed? Why (not)?*
This is possible in principle. This is not a good idea, however, because the views of the model are likely to be ill-formed or inconsistent. If these issues are not fixed, the specification may contain requirements that cannot be satisfied.

Q6.3. *What are the main roles in the STS method? Can some of them be played by the same individual?*
The main roles are the requirements analyst, the risk analyst, and the security engineer. The requirements analyst and the security engineer can be encapsulated into the single role of the security requirements engineer, and played by the same individual. The risk analyst plays a marginal role in the method, and the role can be played without using STS-ml.

Q6.4. *What is the relationship between the STS method and software/system engineering methods?*
The STS method can be used as part of mainstream software/system engineering approaches, and complements them with the socio-technical perspective that is not a primary component in those methods.

Q6.5. *What are the main artifacts that are used in the STS method?*
In addition to the three views that constitute STS-models (social, information, and authorization view), the STS method produces analysis

results when automated reasoning is performed, and the security requirements document that specifies the security aspects of the designed sociotechnical system.

Q6.6. *How is risk analysis embedded within the STS method?*
Risk analysis is included as an external activity; while essential to identify the assets, threats, and their interdependencies, the STS method does not prescribe the use of a specific technique to conduct risk analysis. The risk analyst is free to choose the technique that he deems more adequate for the situation at hand.

Solutions to the Exercises (Chapter 7)

Review questions

Q7.1. *Please determine if the following statements are true or false, and explain why.*

a. Roles can be drawn only in the social view.
False. Roles can be drawn in any of the three views of STS-ml using the STS-Tool.

b. Information entities can be represented only in the information view.
False. They are represented both in the information view and in the authorization view. However, the information view has a more comprehensive representation, which includes their relationships with documents, while their visualization in the authorization view is limited.

c. There can be no redundant authorizations.
False. Authorizations can be redundant, and the automated reasoning techniques that STS-Tool features are able to detect these issues.

d. The tool allows drawing delegation child cycles.
True. It would be overly restrictive to prevent this situation, and it would also require continuous, non-trivial automated checking of the model in background. The modeler can detect whether this situation occurs by explicitly invoking the well-formedness analysis.

e. Security requirements specification documents contain information about security requirements.
True. This type of document contains the entire specification and allows for traceability by showing and describing the STS-ml model that leads to the specification.

f. Security requirements specification documents can be generated only when security needs are expressed.
False. They can be generated at any moment and used as a communication means to interact with the stakeholders.

Q7.2. *Why is the security requirements specification document needed?*
This document is a comprehensive report on the STS-ml model that has been created, and expresses the security requirements that the model includes. It is a single reference point for the stakeholders and analysts to understand the security requirements for the socio-technical system

under design, and comes with explanations that may help reading the diagrams for people who are not familiar with the graphical notation.

Q7.3. *Explain the difference between online and offline analysis in STS-Tool.*
Online analysis includes simple checks of the models that can be performed on-the-fly while the model is being drawn. Offline analysis consists of time-consuming checks that are performed upon explicit user request.

Q7.4. *How does STS-Tool support visual scalability?*
In addition to using three separate views as prescribed by STS-ml, the tool allows for collapsing and expanding the actors, and it makes it possible to hide specific elements from one or more views.

Solutions to the Exercises (Chapter 8)

Review questions

Q8.1. *In Figure 8.1, what is the meaning of the arrow with a "≠" annotation between Tax Agency's goals corporate records created and citizens' records created?*
That arrow indicates a separation of duties requirement specifying that those two goals cannot be achieved by the same agent. Thus, agent Tax Agency has to delegate at least one of them to another actor.

Q8.2. *In Figure 8.1, why is the delegation arrow between TN Company Selector and Okkam Srl dashed?*
The dashing denotes a non-redelegation requirement: the delegatee (Okkam Srl) is in charge of achieving the goal semantic search built and cannot further delegate the goal or its sub-goals to other actors.

Q8.3. *In Figure 8.2, information personal info is owned by Citizen but is made tangible by document personal records, which is in the scope of the Municipality. Is this correct? Why?*
This is correct. In fact, it is a rather common situation that documents are created and possessed by actors that differ from the owners of the information therein. Although personal information (date of birth, name and surname, address) is owned by citizens, municipalities typically are those that can produce the official certificates that represent this information.

Q8.4. *In Figure 8.2, within the scope of actor PAT, both documents residential buildings and land lots are part of document cadastre registry. Does this mean that the registry consists of only those two sub-documents? Why?*
The part-of relationship is read in a bottom-up fashion and it states that a document is part of another. There is no implication on completeness; therefore, there may be other sub-documents as well.

Q8.5. *In Figure 8.3, consider the authorizations for residential address toward InfoTN from actors Tax Agency and Municipality. Are those conflicting? Why?*
The two authorizations that we are considering are the following:

- The Municipality allows reading (among others) the residential address in the context of the goal system maintained, and prohibits (in the same

goal scope) the production of documents that make this information tangible;

- The Tax Agency permits modifying and producing documents that make the residential address tangible in the scope of the goal data refined.

To tell whether those authorizations are conflicting, one has to check in the social view the goals that are mentioned: system maintained and data refined. The second goal turns out to be a subgoal of the first one. As such, the authorizations are conflicting, because the received authorizations give conflicting rights (permit/prohibit) about the production of documents that make data refined tangible.

Q8.6. *Consider the information view in Figure 8.11, and look at the tangible by relationships that link information entities lot geo location and lot info details with document lot info. Note the existence of the part-of relationship between the information entities. Doesn't this imply that the tangible by relationship originating from lot geo location is redundant? Why? Can you think of an alternative modeling?*
The Tangible by relationship that is mentioned above is redundant, although not harmful, because it does not contradict other relationships, and it may be useful to better visualize the model. There are alternative ways to represent the same situation:

- Keeping the model minimal: just remove the Tangible By relationship;
- Removing the part-of relationship from lot geo location and lot info details. This model, however, has a missing parthood relationship; thus, if information lot info details is made tangible by another document, the analyst has to remember to also link lot geo location to that document.

Q8.7. *Consider the information legal info in Figure 8.12. Which actors have rights to modify documents containing such information? For what purposes?*
There are five actors that potentially have rights on information legal info:

- The role Ministry of Law is the information owner. As such, all rights are with agents playing that role;
- The role Solicitor receives an authorization from the Ministry of Law. Specifically, rights are transfered for goal legal frmw provided, in which

context the actor is allowed to read documents and explicitly prohibited from transferring documents.

- The agent DoUP Application rights on legal info are granted by the Solicitor. This second actor is entitled to transfer rights because the authorization received from the Ministry of Law allows for that. The DoUP Application obtains rights to read and transfer documents that make legal info tangible, in the context of the goal citizens helped. This authorization, however, implies at least two violations: (i) the Solicitor is prohibited from transferring legal info and has therefore no rights to authorize others to do so; (ii) the scope for which the authorization is transfered (citizens helped) is not related to the scope the Solicitor has rights on (legal frmw provided).
- The role Real Estate Agency is granted the permission to read documents that make legal info tangible, but is prohibited to modify those documents, in the context of goal legal info added. This authorization cannot be transfered.
- The agent Aggregated REA is transfered rights from the Real Estate Agency. However, the second actor had no rights to do so.

Solutions to the Exercises (Chapter 9)

Review questions

Q9.1. *What is the difference between abuse cases and misuse cases?*
Both approaches are security extensions of UML; misuse cases employ a richer modeling of negative scenarios. An *abuse case* specifies am interaction between an actor and the system that leads to results that are harmful for the system, without employing any specific notation. A *misuse case* represents sequences of actions that a misuser actor or system performs to cause harm in the system, and represents these cases in a black background color. Moreover, misuse cases include two relationships between use cases and misuse cases: the *threaten* relationship indicates that a misuse case threatens the success of a use case, while the *mitigate* relationship specifies that a use case can mitigate a misuse case.

Q9.2. *How do anti-goals relate to STS-ml?*
Anti-goal models study security from the perspective of system attackers at the intentional level. These models can be used as part of threat identification to better understand threats. Unlike anti-goal models, STS-ml focuses on the social relationships among actors and is not limited to the actor-system interactions.

Q9.3. *Are abuse frames suitable for modeling the security aspects of socio-technical system? Why?*
Although a powerful technique to analyze how malicious users can threaten a machine, abuse frames are not focusing on the socio-technical context where machines are located. They focus on the user-machine interaction, and do not explore all the social dependencies between humans and organizations.

Q9.4. *What are the four main elements of SecureUML?*
SecureUML extends UML and enables specifying role-based access control into application models. The four main elements are (i) Roles: the active elements that execute actions in the system; (ii) Entities, the passive elements that the roles use; (iii) Permissions, association classes between a role and an entity that define which methods of the entity a role can invoke; and (iv) Authorization constraints, OCL constraints

that define the conditions under which a permission is granted. These elements are defined as UML stereotypes.

Q9.5. *What are the two main elements of Secure Tropos?*
Secure Tropos features two main security-related concepts: (i) Security constraints are restrictions related to security issues, which influence the design of the system under development; and (ii) Secure entities (goals, tasks, resources), that is, elements that are included in the model to help achieving the security constraints.

Q9.6. *Explain the primitives of SI* that enable representing trust relationships.*
SI* has four primitives for representing trust relationship between two actors A_1 and A_2 in the model: (i) Trust of permission is the expectation of A_1 that A_2 will not misuse a goal; (ii) Trust of execution denotes the expectation of A_1 that A_2 is dependable for achieving a goal; (iii) Distrust of permission indicates the expectation of A_1 that A_2 will misuse a goal; and (iv) Distrust of execution expresses the expectation of A_1 that A_2 is not dependable for achieving a goal.

Q9.7. *What is the difference between the SecBPMN2-ml and the SecBPMN2-Q languages?*
These are the two main components of the SecBPMN2 approach for secure business process design. SecBPMN2-ml enables modeling business processes with annotations that denote security aspects. SecBPMN2-Q is a query language that is used to express procedural security policies that SecBPMN2-ml should comply to.

Q9.8. *Can STS be positioned within the SQUARE method? How?*
SQUARE is a holistic approach for conducting security requirements engineering of technical systems. The STS focuses on the design of a socio-technical system. STS could supports steps 2 and 3 of SQUARE by supporting the definition and refinement of security requirements through the representation of assets and security goals.

Q9.9. *What is the STRIDE model?*
The STRIDE model employs threat modeling to design secure systems by breaking down the system into components, analyzing each component for susceptibility to threats, and mitigating threats. The aim of STRIDE is to discover and detect design problems that potentially allow security breaches prior to the system development phase.