Questionnaire on Security Aspects

Interplay of Human Factors and Secure Architecture Design using Model-Driven Engineering

In the context of a PhD program, we aim to define Human Factors Models characterizing the development team awareness through several different categories related to their direct and indirect human factors.

The awareness of individual team members, and the team as a whole, is characterized based on different human-related factors such as familiarity, capability, riskiness, etc. with respect to technical security mechanisms, policies and procedures, and the adoption of security best practices, for example.

One way in which to build the Human Factors Models is to create a set of development team profiles using the results of questionnaires completed by the development team members involved in the project.

We are conducting a survey to evaluate the security-relevant human factors on the three following security objectives : Confidentiality, Integrity, Availability (**CIA**) using measurements of specific human factors.

In the context of our study, the system architecture is described using the following concepts :

- A **Passive Component** represents components that do not perform any actions in the system by their own volition.
- An **Active Component** represents components performing actions in the system.
- A **Connector** specifies a link that enables communication between interaction points on components by allowing the exchange of communication artifacts.

The questionnaire is composed of four sections : general questions about security, Direct Factors with its three subcategories sections : Skill, Perception, Capability with questions on CIA security objectives.

You will be able to give feedback at the end of the questionnaire.

There are 12 questions in this survey.

General

How many years of experience do you have in security in IT projects ?

❶ Only numbers may be entered in this field.

Please write your answer here:

How many IT projects have you worked on ?

❶ Only numbers may be entered in this field.

Please write your answer here:

Direct Factor - Skill

Did you use Confidentiality (e.g., cryptography,...) mechanisms in your previous projects in the context of :

Please choose the appropriate response for each item:

	Yes, where available (more than 50% of the projects)	Yes, sometimes (between 20 % and 50% of the projects)	Yes, rarely (less than 20% of the projects)	No (0% of the projects)	I don't know
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

Did you use Integrity (e.g., digital signatures,...) mechanisms in your previous projects in the context of :

Please choose the appropriate response for each item:

	Yes, where available (more than 50% of the projects)	Yes, sometimes (between 20 % and 50% of the projects)	Yes, rarely (less than 20% of the projects)	No (0% of the projects)	I don't know
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

Did you use Availability (e.g., filtering,...) mechanisms in your previous projects in the context of :

Please choose the appropriate response for each item:

	Yes, where available (more than 50% of the projects)	Yes, sometimes (between 20 % and 50% of the projects)	Yes, rarely (less than 20% of the projects)	No (0% of the projects)	I don't know
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

Direct Factor - Perception

How did you perceive the Confidentiality (e.g., cryptography,...) mechanisms used in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	Excellent	Good	Satisfactory	To be improved	I didn't faced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

How did you perceive the Integrity (e.g., digital signatures,...) mechanisms used in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	Excellent	Good	Satisfactory	To be improved	I didn't faced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

How did you perceive the Availability (e.g., filtering,...) mechanisms used in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	Excellent	Good	Satisfactory	To be improved	I didn't faced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

Direct Factor - Capability

How have you developed Confidentiality (e.g., cryptography,...) solutions in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	On my own independently	With the help of others (colleagues, external help, internet)	I reused an existing solution off the shelf	I delegated the task to colleagues	I haven't experienced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

How have you developed Integrity (e.g., digital signatures,...) solutions in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	On my own independently	With the help of others (colleagues, external help, internet)	I reused an existing solution off the shelf	I delegated the task to colleagues	I haven't experienced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

How have you developed Availability (e.g., filtering,...) solutions in the majority of your previous project in the context of :

Please choose the appropriate response for each item:

	On my own independently	With the help of others (colleagues, external help, internet)	I reused an existing solution off the shelf	I delegated the task to colleagues	I haven't experienced this problem
Passive Component	○	○	○	○	○
Active Component	○	○	○	○	○
Connector	○	○	○	○	○

Feedback

Feedback on this questionnaire, if there is things to improve, need to be more clear, things you didn't understand or anything else :

Please write your answer here:

Submit your survey.

Thank you for completing this survey.