SAM - Grounded Theory Evaluation Results

Markus Zoppelt Ramin Tavakoli Kolagari

1 Availability

SAM is available as an open source project at
`https://github.com/MarkusZoppelt/SAM`.
The complete metamodel of SAM (including entity descriptions) is also available as an HTML version at
`https://www.in.th-nuernberg.de/Professors/AS2E/SAM/`.

2 Grounded Theory: Code Networks

See figures

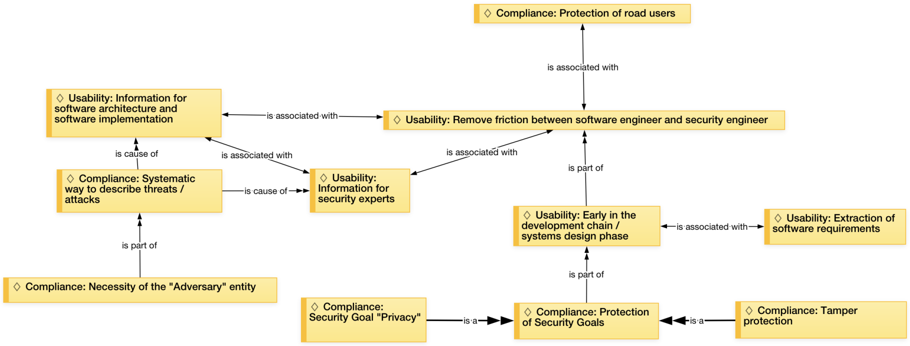
◇ Compliance: Protection of road users
is associated with
◇ Usability: Information for software architecture and software implementation
is associated with
◇ Usability: Remove friction between software engineer and security engineer
is cause of
is associated with
is associated with
is part of
◇ Compliance: Systematic way to describe threats / attacks
is cause of
◇ Usability: Information for security experts
◇ Usability: Early in the development chain / systems design phase
is associated with
◇ Usability: Extraction of software requirements
is part of
is part of
◇ Compliance: Necessity of the "Adversary" entity
◇ Compliance: Security Goal "Privacy"
is a
◇ Compliance: Protection of Security Goals
is a
◇ Compliance: Tamper protection

Figure 1: Code Network: Project Pertinence

3 Grounded Theory: Selected Quotes

Note: The quotes are not edited in any way. The wording matches the transcribed sentences.

Interviewer: "What are your requirements for a secure automotive system? What comes to your mind?"
Expert (security): "Okay, so I guess they should not be tampered with in the way that jeopardize lives and economic values. So, safety and integrity is

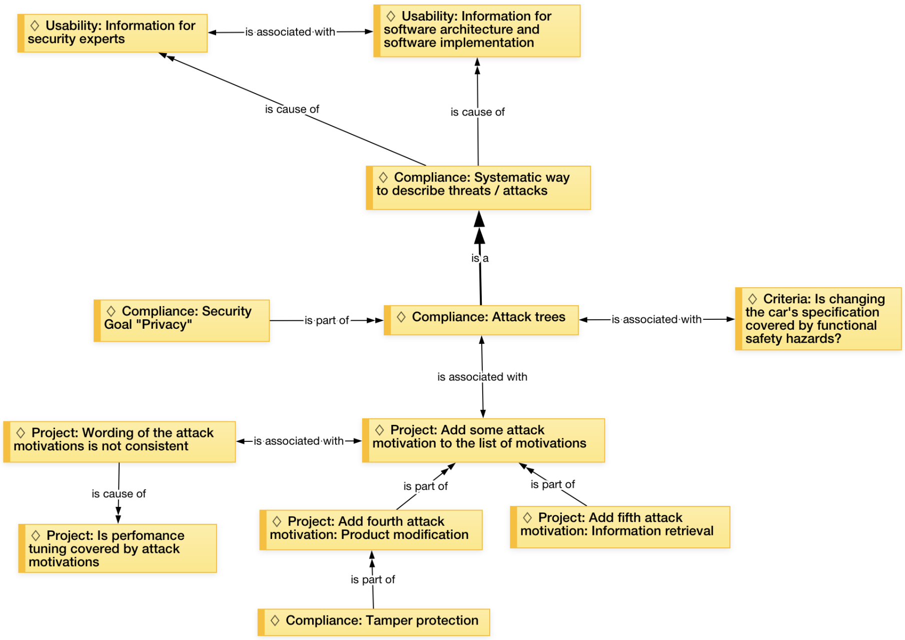
◇ Usability: Information for security experts
is associated with
◇ Usability: Information for software architecture and software implementation
is cause of
is cause of
◇ Compliance: Systematic way to describe threats / attacks
is a
◇ Compliance: Security Goal "Privacy"
is part of
◇ Compliance: Attack trees
is associated with
◇ Criteria: Is changing the car's specification covered by functional safety hazards?
is associated with
◇ Project: Wording of the attack motivations is not consistent
is associated with
◇ Project: Add some attack motivation to the list of motivations
is cause of
is part of
is part of
◇ Project: Is perfomance tuning covered by attack motivations
◇ Project: Add fourth attack motivation: Product modification
◇ Project: Add fifth attack motivation: Information retrieval
is part of
◇ Compliance: Tamper protection

Figure 2: Code Network: Concept Attack Motivations

important. But it should also be secure in the sense that I should not be able to get unauthorized information out of the vehicle or make changes to the vehicle so that it becomes more capable than it was intended or behaves in an illegal fashion. Then we have data protection both in terms of vehicle usage and user behavior. Those should not be able to get access to if not authorized."

Interviewer: "How valuable is SAM to an automotive software engineer?"
Expert (engineering): "To some extend its the system engineer who has derived some software requirements based on that can be diffused from a model like this. So perhaps its main value is early in the development chain. So once to start looking at the software architecture and software implementation as well one will make sure to have this information. The question is how."
Interviewer: "If you have this, it is easy to create attack trees. Its a method that security experts use all the time for modeling threats and attacks. So, if a security expert has this he can easily transform this knowledge and also the category from the attack motivation into attack trees. The attack trees themselves are very useful for identifying and dealing with security threats."
Expert (engineering): "Well I am not sufficiently fluent in security to say. But it could be that most of the conclusions that can be drawn from such an attack tree will result in software requirements that the systems engineer is setting out meaning that the software engineer doesnt have to look into this

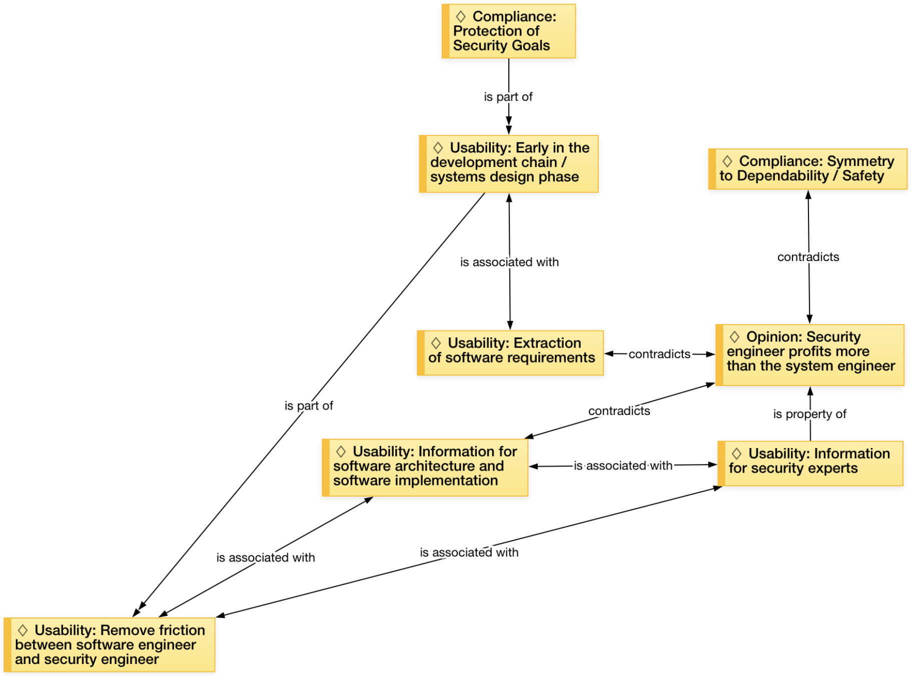
◇ Compliance: Protection of Security Goals
is part of
◇ Usability: Early in the development chain / systems design phase
◇ Compliance: Symmetry to Dependability / Safety
is associated with
contradicts
◇ Usability: Extraction of software requirements
contradicts
◇ Opinion: Security engineer profits more than the system engineer
is part of
contradicts
is property of
◇ Usability: Information for software architecture and software implementation
is associated with
◇ Usability: Information for security experts
is associated with
is associated with
◇ Usability: Remove friction between software engineer and security engineer

Figure 3: Code Network: Industry Acceptance

information structures too much."

Interviewer: "Does the concept of categorizing the attack motivation make sense to you? Would you add some new category?"
Expert (security): "They seem pretty complete from a security stand point. FinancialGain is most important in my opinion. But I guess they are somewhat linked. Some attacks can have more than one motivation. Every PrivacyInvasion is also a FinancialGain. But I see that SAM covers this, that's good. In my opinion the differentiation makes only sense from a technical point of view."

Interviewer: "How valuable is this extension to a security expert?"
Expert (engineering): "It seems like a way to organize the threats to deal with them in a systematic way. It seems very useful for that role. And then the systems expert would be the one to define requirements to mitigate back I suppose. They would surely benefit from this information."

Interviewer: "Does SAM help to bring security experts and system engineers closer together? Because they have a common base to exchange information now."
Expert (engineering): "Yeah, I guess the main stakeholder is the security engineer rather than the system engineer because with Dependability it starts

with the Safety Engineers defining the SafetyGoals and then they can work on a functional safety concept to give to the system engineer but it would be similar to security, but I suppose you need a functional security and technical security concept. That could be a way to show more clearly what the role the requirement has.”

4 Grounded Theory Code Table

Symbol	*Meaning*
++	High agreement or interest (more than 50% of experts agreed)
+	Notable agreement or interest (roughly 50% of experts agreed)
o	Moderate agreement or interest (less than 50% of experts showed interest)
-	Limited agreement or interest (roughly 50% of experts disagreed)
--	Low agreement or interest (more than 50% of experts disagreed)
+/-	Mixed agreement or interest (experts were of different opinion)

Table 1: Symbol key for the evaluation results table.

Categories and codes	*Results*
Project pertinence	
Need for protection of road users	++
Need for removing friction between software engineers and security experts	++
Systematic way to describe threats / attacks	+
Extraction of software requirements	++
Necessity of the “Adversary” entity	o
Need for protection of security goals	++
SAM concept and attack motivations	
Information for software architecture and software implementation	++
Systematic way to describe threats / attacks	+
Use of attack trees	+
Completeness of attack motivations	+
Wording of attack motivations	+/-
Acceptance in the industry	
Usability early in the system design phase	++
Symmetry to dependability / safety	++
Information for security experts	++
Information for software engineers	-

Table 2: Summary of the evaluation results.