Specifying Reusable Security Requirement

Donald Firesmith

Presented by Rex

Summary

- In the paper, author pointed out the basic concept of what is security requirement.
  - Quality factors and sub factors
  - Identification and authentication mechanisms
- He also explained the benefit of reuse security requirement and given some example.
  - Benefit for engineer with no training and non expert
  - Sure the quality of that requirement.
- Finally, he talked about asset-based and risk-driven approach when analysis.
  - What do we want to protect and what negative impact will face if fail.

Why reuse security requirement?

- For same category of system, although they are different but if they are similar, they may have same requirement on security. Reuse security requirement template can improve the processing more effective.
- Some benefit by reuse security requirement:
  - Easier for new developer or engineer.
  - Sure on valuable and feasible.
  - Faster than build on nothing.
  - Less miss or error.

My comment

- Using templates like the below picture may still to hard for less skilled programmer and or non-expert engineer. We can improve it to be smarter by including some up-to-date AI and database techniques.

"The [application / component / data center / business unit] shall protect the [identifier | type] data it transmits from corruption (e.g., unauthorized addition, modification, deletion, or replay) due to [unsophisticated / somewhat sophisticated / sophisticated] attack during execution of [a set of interactions / use cases] as indicated in [specified table]."

– [Table of interactions / use cases versus minimum acceptable measurement level].

Basic idea

- In the paper, it states “The high potential reusability of security requirements is very beneficial because most requirements engineers have had no training in identifying, analyzing, specifying and managing security requirements and most requirements teams do no include subject matter experts in security.”

- Template is good idea for the programmer or engineer talked in above statement. But they still need some skill to use template when face some complex and difficult system.

So, What can we do?

- I figure we can improve the reuse those requirement rather than fill in the form.
  - Wizard
  - Search Engine and Forum

Wizard

- Wizard would ask engineer some question base on asset-based and risk-driven approach to make a decision on what security level and requirement would be needed. And use AI engine to find out some requirements in similar system.

- Example question:
  - What type of system?
  - What type of information would be protected?
  - Any confidential information will disclose when security fail?
  - What is the possibility amount of loss in term of money when security fail?
  - Will a new war happen when security fail?

Wizard (Advantage and Disadvantage)

- Advantage:
  - The most easy way to build up some basic security engine by less skilled people.
  - Less time on research and model.
- Disadvantage:
  - Can AI found a result as good as human expert?
  - Can AI can found a good result for a system with complex structure?
  - AI engine need lots of successful case to be example for build a good result.

Search Engine or Forum

- Programmer and engineer types in keywords about the system in search engine and gets back related security requirements in similar system developed by other people before. Also, Programmer and engineer can share their comments for those security requirements in the database or submit their own work too.

- Example: Search engine like Google and lots of forum about Security.

Search Engine or Forum (Advantage and Disadvantage)

- Advantage:
  - Programmer and engineer can find lots of related security requirement in short time.
  - They can receive the feedback of their own work from other skilled people too.
  - Open area means information can improve day by day.
- Disadvantage:
  - Need lots of visitor to build up a successful area
  - Sometimes search engine would reply lots of rubbish
  - Open area also means you can’t prove the quality of the search result.

Question for discussion

- Are there any other techniques we can use to help less skilled people to build security easier?
- What is the possibility of building a security code engine fit different security requirement, similar to code libraries for mathematical and physical engines?