Turn Around Security SM

AppSec Designer™ Information Sheet

Eliminate Security Design Errors in Software that Contribute up to $166 Billion in Losses Each Year

Worldwide losses due to cyber security vulnerabilities are $500 Billion per year. In MITRE's Common Weakness Enumeration, one-third of software vulnerabilities are described as design errors. These may account for up to $166 Billion in losses per year.

AppSec Designer™ Introduces a New Paradigm:

- Common Criteria Security Functional Requirements, including their dependencies, are re-used and grouped into Security Requirements Packages
- Security Components are characterized as consisting of Security Requirements Packages
- Reference Libraries are community-supported, and may be customized locally to meet your needs and standards
- This enables expanding, e.g., a TLS Component into over 25 detailed Application Security Functional Requirements
- AppSec Designer™ uses Graph Database technology which enables enumerating a large number of Application Security Functional Requirements very fast
- Application Security Functional Requirements can now be enumerated:
    - At the low-level logic-layer of a design
    - For a very large number of requirements
    - At very fast speeds
    - In such detail that Threat Modeling becomes less relevant
- This completely changes how Security Architects, Security Engineers, and Developers can obtain Security Requirements
- Business Nonfunctional Security Requirements typically are not very effective from a security design perspective, and they do not tell the programmers how to incorporate security functions into designs. With AppSec Designer™ they can generate useful Application Security Functional Requirements that they can program to
- Better yet, the Application Security Functional Requirements can be provided to QA testers. They will be able to test security design details that were previously omitted

Benefits of AppSec Designer™

- Enables characterizing security variables in a model so they can be controlled
- Expands the security requirements using community-supported Security Functional Requirements libraries, and their dependencies
- By selecting which Application Security Functional Requirements are already implemented in the current design, the missing requirements are identified
- Enables standardizing the Threat Modeling process, selection of countermeasures, and the related security functional requirements – using a community-supported threat modeling and countermeasures library
- Slash your software security liability by up to 1/3rd
- Facilitates decision-making using Risk-Benefit Analysis of each missing security functional requirement, generating documentation where risk is accepted
- Supports deferring implementation of missing security functional requirements, and documenting which application release the changes are deferred to
- Facilitates generating reports needed to implement missing requirements – for design and coding changes, plus unit, integration, and QA testing
- Provides details for system security plans in ISO and NIST formats

Licensing Available (estimated availability 2Q 2018)

- Free online service (limited to a single application model at a time) that makes use of community provided and supported security functional requirements and threat modeling mitigations libraries
- Single user license
- Enterprise license

Turnaround Security, Inc. · 9841 Washingtonian Blvd · Suite 200 · Gaithersburg MD 20878 · (240) 720-7678

For more details, email Info@TurnaroundSecurity.com

TurnaroundSecurity.com