

УДК 004.056

Є.В. Тиш, канд. техн. наук, Е.В. Шамрай

Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПІДХІД SAFETY CASE ЯДЕР ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ WEB-SERBERІВ

Ie.V. Tysh Ph.D, E.V. Shamray

SAFETY CASE CORE APPROACH FOR WEB SERVERS SECURITY PROVIDING

Під Safety Case інфраструктурою розуміють комплекс всіх взаємопов'язаних Safety Case ядер, задіяних при оцінюванні конкретної системи, в сукупності з іншими методами аналізу, використаними для дослідження функціональної безпеки web-серверів. Однією з важливих особливостей Safety Case інфраструктури є її гнучкість і масштабованість. Кількість Safety Case ядер, задіяних при оцінюванні системи не є фіксованою. Кількість може змінюватися при еволюції системи, додаванні нових елементів, зміні вимог, а також при опрацюванні та вдосконаленні самого процесу оцінювання, виділенні нових Safety Case ядер або декомпозиції вже існуючих ядер на кілька ядер нижнього рівня для більш вузьконаправленого і детального аналізу.

На основі результатів, одержаних на виході всіх використовуваних Safety Case ядер складається загальний документ обґрунтування безпеки web-серверів. Чим більш деталізованою буде декомпозиція системи, більшу кількість Safety Case ядер застосовано і більше факторів ризику враховано, тим більш достовірним буде отриманий результат і більш детальним буде побудоване обґрунтування безпеки системи в цілому.

Внутрішня структура та склад ядра можуть бути різними для ядер, що реалізують різну функціональність. Для будь-якого ядра незмінним залишається алгоритм оцінювання певних показників або характеристик, представлений у формалізованому вигляді. Крім основного компонента, до складу ядра може входити ряд додаткових елементів.

До складу Safety Case ядра можуть входити:

- набір вхідних параметрів, що представляє собою характеристики або вимоги, на відповідність яким можливо провести перевірку за допомогою даного ядра;
- алгоритм перевірки або оцінки на відповідність заданим параметрам / вимогам, який повинен бути представлений у формалізованому вигляді. Цей компонент є обов'язковою складовою ядра;
- програмна логіка побудови і візуалізації алгоритму оцінювання, в залежності від визначених вимог. Наприклад, представлення алгоритму оцінювання у вигляді Ascad або GSN нотації, з додаванням тверджень для заданих вхідних параметрів;
- інтерфейси і логіка взаємодії з наявними даними про систему;
- додаткові матеріали (таблиці значень, бази даних), якими оперує ядро. Ці дані зазвичай ставляться до певної вузькоспеціалізованої області функціональності ядра;
- програмний код обчислення параметрів, перевірки на відповідність вимогам та програмно реалізованої внутрішньої функціональності ядра;
- модулі побудови графіків і візуалізації результатів;
- модулі генерації тексту для Safety Case документів.