Wykazywanie dowodów: Zarządzanie Dowodami na Ukierunkowane Normy Bezpieczeństwa Oprogramowania

Vivien Hamilton

Viv Hamilton Associates Ltd Wethersfield, Essex, UK

Streszczenie. Ukierunkowane standardy bezpieczeństwa wymagają podejścia opartego na dowodach ze strony dostawców oraz dużej ilości dowodów na zapewnianie bezpieczeństwa, które jest generowane przez wymogi projektowanego oprogramowania w zakresie skutecznej oceny i zarządzania. Należy w sposób zorganizowany przeprowadzić dyskusję i ustalenia z ciałami wydającymi rozporządzenia i innymi zainteresowanymi stronami na wczesnym etapie cyklu życia projektu, tak aby procesy projektu były projektowane w sposób mogący przynieść wymagane dowody. Ta dyskusja nt. bezpieczeństwa musi być prowadzona na poziomie wystarczająco abstrakcyjnym tak, aby określić wymagania dotyczące dowodów nie próbując wyraźnie określić konkretnych dowodów do wygenerowania. Należy zapewnić sposób identyfikowalności pomiędzy wymogiem abstrakcyjności dotyczącym dowodów, a konkretną realizacją potrzeb, które należy zapewnić: baza danych SQL, która może mieć hiperłącze do argumentu, jest skutecznym środkiem zarządzania zarówno statusem dowodów jak i identyfikowalnością (spójnością pomiarową) argumentu o bezpieczeństwie. Sprawa bezpieczeństwa jest zakończona, gdy dowód został pomyślnie wygenerowany i oceniony w raporcie dowodowym, w którym można skutecznie zarządzać oceną ograniczeń dowodów i dowodów przeciwnych może być.

1 Wstęp

Niniejsze opracowanie dotyczy praktycznych zagadnień zarządzania dowodami tworzonymi w trakcie pracy nad budową dużych systemów oprogramowania i wymaganymi w ramach kwestii bezpieczeństwa, zanim oprogramowanie może zostać oddane do użytku. Szereg prac naukowych omawiało już kwestie bezpieczeństwa, ale bardzo niewiele zajmowało się konkretnie dowodami. Niniejszy artykuł ma głównie zastosowanie do projektów zajmujących się na ukierunkowanymi standardami, takimi jak Norma Obronna 00-56 (MON 2007) i WE 482/2008 (Komisja Europejska 2008) w kontroli ruchu lotniczego, który jest realizowany w SW01 w Wielkiej Brytanii (Civil Aviation Authority 2010). Standardy te nie mają charakteru nakazowego co do tego, jak bezpieczeństwo oprogramowania jest osiągane, ale wymagają natomiast zorganizowanego argumentu o bezpieczeństwie, popartego dowodami, dlaczego produkt w postaci oprogramowania jest bezpieczny i wygenerowany w ramach ogólnego systemu zarządzania bezpieczeństwem. Oczywiście, duże ilości dowodów są także generowane przy spełnianiu innych standardów, więc niektóre z zagadnień omawianych w niniejszym opracowaniu mogą być istotne dla projektów stosujących bardziej normatywne (nakazowe) standardy procesowe, takie jak DO-178B (RTCA 1992) lub IEC 61508 (IEC 2000).

C. Dale T. Anderson (red.), Postępy w systemach bezpieczeństwa, DOI 10.1007 / 978-0-85729-133-2_3,

Ukierunkowane normy wymagają podejścia opartego na dowodach od dostawcy (Hamilton 2006) ponieważ, chociaż to argumenty porządkują i nadają sens dowodom, to właśnie dowody zapewniają pewność. Ostatecznie w kwestii bezpieczeństwa musi zostać stwierdzone, że istnieją wystarczające dowody na to, aby wykazać, że produkt jest w sposób akceptowalny bezpieczny.

W małym projekcie ilość dowodów jest bardziej identyfikowalna, ale gdy zakres prac nad rozwojem i weryfikacją oprogramowania może wynosić w setki osobo-lat, dowody generowane przez te procesy będą adekwatnie duże, a wysiłek potrzebny do zagwarantowania, że dowody są właściwie oceniane może być nadmierny.

W kontekście systemu regulacyjnego, który wymaga, aby ryzyko było na poziomie ALARP (najniższe jak to będzie praktycznie możliwe), istnieje domniemany wniosek, że nakład w celu uzyskania pewności musi być stosowany tak skutecznie, jak to możliwe, ponieważ jeśli jest nieefektywny, lub zawiera wysiłek bezskuteczny, taki zmarnowany wysiłek mógł być potencjalnie zastosowany w innym miejscu w celu osiągnięcia dalszej redukcji ryzyka. Efektywne zarządzanie dowodami jest niezbędne do osiągnięcia tego celu, podobnie jak potencjalnie zapewnianie oszczędności w ramach projektu i upewnienie się, że zatwierdzenia organów nadzoru mogą być uzyskane na czas.

2 Zarządzanie argumentem

Argument o bezpieczeństwie jest złożonym elementem analizy, który musi być kontrolowany i sprawdzany pod kątem ważności w sposób manualny. Chociaż wprowadzenie notacji strukturyzujących, takich jak *Notacja strukturyzująca cel* (GSN) (Kelly 1999) i *Dowody argumentacji roszczeń* [Claims Argument Evidence] (CAE) (Adelard 1998), pozwala na bardziej rygorystyczne analizowanie argumentu, weryfikacja poprawności argumentu nadal wymaga recenzji sporządzanej przez ludzi. Argument musi zatem być przedstawiony w sposób, który promuje jego czytelność. Argument, który jest zaśmiecony szczegółami jest trudny do zrozumienia i zawiera ryzyko, że będzie rozpatrywany w sposób fragmentaryczny, tak, że interakcje zachodzące w różnych interakcjach częściach argumentu pozostaną niezauważone. W zarządzaniu argumentami i dowodami, inżynieria bezpieczeństwa musi wyciągnąć wnioski z inżynierii oprogramowania i przyjąć zasady abstrakcji oraz oddzielania wymagań od realizacji: argument musi zdefiniować wymagania dla różnych rodzajów dowodów abstrahując od szczegółów realizacji dowodów. Takie podejście umożliwia to, aby argument (potwierdzenie) bezpieczeństwa mógł być wytwarzany i uzgadniany na wczesnym etapie cyklu życia, ale w celu zakończenia sprawy bezpieczeństwa, sprawozdania dot. dowodów, które śledzi procesy „z powrotem” do takiego argumentu, będą musiały być sporządzane na końcu procedury zapewniania wiarygodności.

Dodatkowym problemem w zakresie uzyskania zgody co do potwierdzenia (argumentu) bezpieczeństwa jest to, że zazwyczaj wymagana jest zgoda wielu zainteresowanych stron, w tym organu nadzoru, organu operacyjnego, integratora systemów, producenta oprogramowania i niezależnego eksperta w dziedzinie bezpieczeństwa. Ponadto argument o bezpieczeństwie jest kluczowym dokumentem zarówno dla bezpieczeństwa i ryzyka projektu, więc jest prawdopodobne i pożądane, zwłaszcza biorąc pod uwagę nacisk kładziony w niniejszym opracowaniu na duże projekty zajmujące się oprogramowaniem, aby posiadać zatwierdzenia wyższych urzędników w każdej z zaangażowanych w projekt organizacji. Jest wysoce pożądane, aby argument był uzgadniany na wczesnym etapie cyklu życia, a najlepiej w ramach etapu planowania obok tworzenia planu zarządzania bezpieczeństwem i planów technicznych, takich jak plany rozwoju oprogramowania i weryfikacji: jeśli będzie nieco później, wzrośnie trudność w zakresie potrzeb zapewnienia bezpieczeństwa, aby wpływać na działania rozwojowe i weryfikacji. Stworzenie zwięzłego argumentu, to jest ograniczonego do wymogów w zakresie dowodów, które mają być wyprodukowane i unikanie szczegółów realizacji powinno ułatwić osiągnięcia takiego porozumienia na wczesnym etapie. Co więcej, wymagania dot. dowodów mogą być w takiej sytuacji określone jako cele w zakresie rozwoju oprogramowania i procesów weryfikacji, zaś szczegóły, w jaki sposób zostanie wygenerowany i przedstawiony taki materiał dowodowy mogą następnie wyłonić się z projektowania procesów oprogramowania. Jest to o wiele bardziej wydajne niż posiadanie zespołu bezpieczeństwa dyktującego szczegółową formę dowodów dla inżynierów oprogramowania, co może prowadzić do niepotrzebnych zmian dokonywanych w ustalonych i dojrzałych procesach dostawcy oprogramowania.

Duża liczba podmiotów, które są zazwyczaj zobowiązane do uzgodnienia potwierdzeń (argumentu) bezpieczeństwa oznacza, że ich aktualizowanie może być kosztowne i czasochłonne. Zmiany w zakresie argumentu bezpieczeństwa mogą być nieuniknione, na przykład, jeśli w trakcie rozwoju systemu pojawiają się nowe wymagania bezpieczeństwa lub ograniczenia dotyczące bezpieczeństwa, jeśli odkryta zostanie znacząca ilość dowodów przeciwnych, lub jeżeli zamierzone procesy projektowania i wdrażania ulegają znaczącej zmianie. Jednakże, dobrym argument bezpieczeństwa musi być napisany w sposób, który oznacza, że drobne zmiany mogą być „absorbowane” przez szczegóły dostarczenia dowodów, tak, że tylko istotne zmiany wymagają wprowadzania także stosownych zmian do argumentu. Argument o bezpieczeństwie będzie musiał odnieść się do raportu dowodowego w kwestii bezpieczeństwa i ponieważ, jak to opisano w dalszej części niniejszego opracowania, raport taki omawia ograniczenia w dowodach i dowodach przeciwnych, to odniesienie do sprawozdania dowodowego stanowi kolejny przykład abstrahowania od zbędnych szczegółów, czyniąc argument o bezpieczeństwie odpornym na drobne niespójności w dalszych procesach generowanych dowodach.

Biorąc pod uwagę, że argument powinien dotyczyć jedynie abstrakcyjnych wymagań w zakresie dowodów, potrzebne będą sposoby identyfikowania tych wymogów z konkretnymi realizacjami dowodów. Prostą metodą jest sposób, aby argument identyfikował symbole zastępcze w systemie zarządzania konfiguracją: te symbole zastępcze mogą być później wypełnione albo pojedynczym dokumentem lub hierarchią folderów i dowodów. Jednakże, bardziej satysfakcjonujące podejście polega na korzystaniu z relacyjnej bazy danych, aby powiązać węzły argumentu z elementami dowodowymi. Zaletą bazy danych jest to, że może ona pomieścić dodatkowe metadane: np. osoba odpowiedzialna za tworzenie dowodów, data utworzenia, jej stan pod względem kompletności, a także w zakresie oceny w stosunku do argumentu. The Object Management Group (OMG) niedawno wygenerowała standardowy schemat dla argumentów o bezpieczeństwie jako Software Assurance Evidence Metamodel (SAEM) [metamodel dowodu dla zapewniania jakości oprogramowania] (Object Management Group 2010). Baza danych, która jest dostępna przez

hiperłącza, np. realizowana w SQL, można także włączyć hiperłącza do wpisów w bazie danych dla dowody mających być osadzonych w argumencie (potwierdzeniu).

3 Zarządzanie procesami tworzącymi dowody

Jak już wspomniano, argument bezpieczeństwa musi być uzgodniony na możliwie najwcześniejszym etapie projektu. Aby zrozumieć, co należy potwierdzać, kwestie inżynierii i oceny istotnych systemów bezpieczeństwa muszą zostać podjęte zanim można stworzyć potwierdzenia bezpieczeństwa, ale pożądane jest, aby argument pojawił się już na etapie planowania przed rozwojem oprogramowania. To gwarantuje, że procesy, które generują największe ilości dowodów (szczegółowa specyfikacja oprogramowania; rozwój oprogramowania; weryfikacja oprogramowania, weryfikacja i walidacja systemu) mogą być zaprojektowane do przedstawienia dowodów, które są stosowne dla celów zapewnienia gwarancji.

Abstrakcyjne wymagania dla dowodów, jak podano w argumencie o bezpieczeństwie powinny być wyraźnie określone w dokumentach, które określają procesy, które generują te dowody: np. odniesienia w argumencie o bezpieczeństwie do identyfikacji i oceny zagrożeń będą prawdopodobnie obsługiwane przez procesy inżynierii bezpieczeństwa; odniesienie do demonstracji zachowań oprogramowania przypuszczalnie będzie obsługiwane przez procesy testowania lub analizy oprogramowania. Określając wymagania dotyczące dowodów jako cele procesu, można zaprojektować dany proces jako przeznaczony do generowania dowodów w wymaganej formie, zaś weryfikacja dopuszczalności dowodów może być normalną częścią weryfikacji procesu. Ma to również dodatkową korzyść, a mianowicie taką, że każdy członek projektu może zobaczyć, jak jego praca przyczynia się do produkcji bezpiecznego (i gwarantującego jakość) produktu.

W poprzednim artykule (Hamilton 2006) zastanawiano się, jakie są dwa rodzaje właściwości dowodów: te, które mogą być obiektywnie ocenione i te, które są przedmiotem oceny (ekspertów). Procesy mogą często być określone w taki sposób, że wiele obiektywnych właściwości dowodów uzyskuje się automatycznie. Na przykład, w inżynierii oprogramowania środowisko programistyczne może być skonfigurowane tak, aby prawidłowo nazwane obiekty były przechowywane w systemie zarządzania konfiguracją z odpowiednimi polami metadanych wypełnionymi. Przykładem z inżynierii bezpieczeństwa może być narzędzie do wspierania HAZOP, które zapewnia, że wpisy są rejestrowane dla wszystkich haseł/słów-kluczy (*guidewords*) ze zdefiniowanego ich zbioru. Właściwości, które są przedmiotem oceny, nie można w ten sposób zautomatyzować, na przykład obiekt inżynierii oprogramowania będzie musiał zostać poddany przeglądowi w celu zapewnienia, że jest odpowiednio zaprojektowany, zaś HAZOP będzie musiał zostać poddany przeglądowi w celu zapewnienia, że wszystkie wpisy są prawidłowe i mające znaczenie; jednakże, może wciąż być możliwe zapewnienie wsparcia narzędziowego w celu zapewnienia ścieżki audytu, na przykład w celu wymuszenia, aby osoba o określonej roli uzupełniała pole przeglądu. Z perspektywy dobrej inżynierii bezpieczeństwa, dowody oraz ocena dowodów powinny być jak najbardziej obiektywne. Nie jest możliwe, aby fachowa oceny ekspercka została całkowicie usunięta, ale powinna być ona oparta tylko na tych właściwościach dowodów, które są koniecznym przedmiotem oceny. Argument, który korzysta z subiektywnego osądu obiektywnych właściwości, które można było obiektywnie ocenianych, może jawić się jako “nieznaczący" i nieprzekonujący. Aby upewnić się, że te obiektywne właściwości mogą być obiektywnie ocenione, należy zaprojektować procesy tak, aby systematycznie dostarczały one dowodów i weryfikowały ich właściwości.

W notacji CAE dot. spraw bezpieczeństwa, dowody są związane z roszczeniami poprzez argumenty które wyraźnie uzasadniają, dlaczego dowody są wystarczające do odrzucenia roszczenia. GSN nie ma tak wyraźnego argumentu: ma za to opcjonalną notację uzasadniającą, ale ogólnie rzecz biorąc cele powinny być rozłożone na części na tyle, aby relacje między dowodami i celami były oczywiste. W obu przypadkach należy się zastanowić, dlaczego dowody są wystarczające do spełnienia roszczeń bezpieczeństwa, dlaczego to podejście zostało wybrane, i jak zostały rozwiązane kwestie potencjalnych niedociągnięć. Są to także pytania, które należy uwzględnić przy planowaniu procesów, które zostaną przyjęte w projekcie, więc dokument, który zawiera definicję procesu jest również oczywistym miejscem do zapisu uzasadnienia podejścia, mając na uwadze z poprzedniej dyskusji, że dokument procesowy powinien wyraźnie określać, jako cele procesu, wymagania dla dowodu zdefiniowanego w argumencie (potwierdzeniu) bezpieczeństwa. Tak więc na etapie planowania projektu, inżynier ds. bezpieczeństwa powinien aktywnie uczestniczyć w dyskusji z każdy z innym ekspertem w ramach projektu, obejmując projektowanie oprogramowania, kodowanie, testowanie itd., aby zapewnić, że każda definicja procesu spełnia potrzeby zapewnienia bezpieczeństwa obok innych celów technicznych projektu.

Istnieje jeden dodatkowy obszar, w którym procesy projektowe mogą być optymalizowane w celu dostarczenia dowodów w postaci odpowiedniej dla kwestii bezpieczeństwa, i który znajduje się w ostatecznej postaci dokumentacji. Każdy proces po zakończeniu projektu powinien wyprodukować jakąś formę dokumentu podsumowującego, potwierdzającego ukończenie procesu, osiągnięcie celów procesu (w tym celów wygenerowania dowodów na zapewnienia bezpieczeństwa), a także wyraźnie odwołującego się do zasobów dowodowych uzyskanych w wyniku tego procesu. Oczywiście, większość projektów robi to już przy testowaniu, ale nie jest to koniecznie regułą, że istnieje taki raport zbiorczy podsumowujący dla specyfikacji, projektu i procesów kodowania. Przy małym projekcie może nie być takiej kwestii: jeśli, na przykład, cała specyfikacja może zostać objęta jednym dokumentem, wówczas ostatnie wydanie dokumentu pośrednio dostarcza takiego dokumentu. W dużym projekcie jednakże, specyfikacja może najprawdopodobniej zostać rozłożona na wiele dokumentów i to, co ma być wydane lub zaktualizowane jako ostatni taki dokument, odnosi się tylko do jednego obszaru oprogramowania i nic nie mówi o procesie specyfikacji jako całości. Nałożenie dodatkowego wymogu sporządzenia takiego dokumentu podsumowującego zapewnia dogodny sposób uproszczenia identyfikowalności od argumentu do materiału dowodowego. Ma też tę zaletę, że oficjalne dokumenty zazwyczaj posiadają określony proces przeglądu i zatwierdzania dokumentów z sygnatariuszami, zatem taki formalny dokument oferuje sposoby generowania dowodów, które odpowiednie osoby, zarówno kompetentne, jak i odpowiedzialne za dostarczenie części dowodów, potwierdziły, jako dowody poprawne.

Rysunek 1 przedstawia, w jaki sposób odniesienie do dowodów, za pomocą dokumentów podsumowujących i definicji procesów, które uzasadniają ten proces, może wyglądać w argumencie o bezpieczeństwie zbudowanym przy użyciu GNS.

Rys. 1. Przykład argumentu używającego cele bezpieczeństwa odnoszące się do GSN w celu przetwarzania definicji i podsumowujących dokumentów dowodowych

4 Ocena dowodów

4.1 Ogólny proces oceny

Proces oceny powinien zapewnić, aby ocena była jak najbardziej obiektywna, i aby wszelkie anomalie, ograniczenia, deficyty zabezpieczeń oraz w dowody przeciwne były rozpatrywane w sposób przejrzysty i na odpowiednim etapie takiej oceny. Inżynieria oprogramowania wykorzystuje model V do zbadania relacji między wymaganiami a wdrażaniem, oraz między ewidencją testową wygenerowaną na kolejnych etapach integracji, zaś podobny model może pokazać, jak dowody powinny być stopniowo poddawane ocenie.

Rysunek 2 ilustruje, z lewej strony, jak wymogi dotyczące dowodów są wydobywane z argumentu bezpieczeństwa poprzez definicje procesów, które generowały te dowody. Z prawej strony widać stopniowe oceny poszczególnych elementów dowodowych w stanie surowym, do ogólnej oceny akceptowalności (lub nie) kwestii bezpieczeństwa. Każdy pojedynczy element dowodowy jest najpierw weryfikowany pod kątem kryteriów zakończenia procesu co do uzyskania pozytywnych / negatywnych wyników, np. czy wynik badania mieścił się w obrębie określonych tolerancji, czy plik z kodem przeszedł kontrolę analizy statycznej, czy dokument projektowy pomyślnie przeszedł swój proces przeglądu? Dla większości z tych ocen stawiane są obiektywne kryteria określone w definicji procesu; weryfikacja jest normalną częścią procesu i angażowanie ekspertów ds. bezpieczeństwa nie powinno być konieczne.

Rys. 2. V diagram prezentujący relację pomiędzy celami dot. dowodów a etapami oceny

Dokument podsumowania proces określa następnie, w jakim stopniu wyniki tego procesu spełniły cele bezpieczeństwa. Czy wszystkie testy zdały? Jeśli nie, to jaki był wskaźnik zdawalności i gdzie są rejestrowane i analizowane błędy? Czy wszystkie testy zostały przeprowadzone dokładnie tak, jak to zostało określone? Jeśli nie, jakie były odchylenia i jakie są konsekwencje dla celów bezpieczeństwa? Zostały wszystkie testy zostały zakończone? Jeśli nie tam, gdzie stwierdza się, które części oprogramowania nie są testowane? Ponieważ ta część oceny dowodów dotyczy zgodności procesu, dodatkowe wspomagające dowody w kwestii bezpieczeństwa mogą być dostarczone przez badanie jakości, aby sprawdzić, że procesy są właściwie przeprowadzane.

Zarówno Norma Obronna 00-56 i WE 482/2008 wymagają argumentu o bezpieczeństwie, aby umożliwić opracowanie w ramach systemu zarządzania bezpieczeństwem. Obiektywne dowody w zakresie prawidłowego funkcjonowania systemu zarządzania bezpieczeństwem, a także systemu zarządzania jakością projektu powinien być również rejestrowane i podsumowane, należy również przeprowadzić audyty w celu potwierdzenia skuteczności tych systemów zarządzania. Zakładając, że system zarządzania jakością zawiera metody zarządzania odchyleniami procesów od norm, i że system zarządzania bezpieczeństwem zawiera systemy zarządzania potencjalnymi problemami w zakresie bezpieczeństwa w produkcie lub wykazanymi w materiale dowodowym, wtedy one też są procesami, które należy podsumowywać, z rejestrowaniem każdego zaobserwowanego ograniczenia.

Tytuł tego artykułu brzmi *wykazywanie dowodów*, ponieważ odzwierciedla on fakt, że to, co powinno mieć miejsce, polega na systematycznym rejestrowaniu i obiektywnej ocenie. Ponadto, wszystkie ograniczenia w zakresie dowodów powinny być rejestrowane, tak, aby ogólna prezentacja dowodów pokazywała w sposób przejrzysty dokładnie to, co zostało osiągnięte, a co jeszcze pozostało niesprawdzone. Ponieważ procesy kontynuowane są w górę po prawej stronie modelu V, wymagane jest więcej oceny w zakresie bezpieczeństwa przy szacowaniu wpływu na sprawy bezpieczeństwa poszczególnych wad i ograniczeń odkrytych w szczegółowym materiale dowodowym.

4.2 Ograniczenia, dowody przeciwne, oraz braki ubezpieczeń /deficyty pewności/

Życie nie jest doskonałe, i podobnie rzecz ma się z dowodami. Oprogramowanie będzie zawierać błędy; będą nieudane testy; dokumentacja będzie zawierać błędy, a audyty znajdą odchylenia od norm w procesach. Problemem z perspektywy oceny kwestii bezpieczeństwa jest to, w jakim zakresie te niedoskonałości rzeczywiście będą ważne dla bezpieczeństwa.

W tym artykule słowo *ograniczenie* (limitations) zostało użyte jako ogólne określenie opisujące różnicę jaka występuje w relacji do idealnego stanu dowodowego. *Dowody przeciwne* (counter-evidence) zostały zdefiniowane w Normie Obronnej 00-56 jako dowody *z potencjałem* do podważenia roszczeń w zakresie bezpieczeństwa. Ponieważ Norma Obronna 00-56 wymaga aktywnego poszukiwania dowodów przeciwnych, to ograniczenie należy uznać za możliwy dowód przeciwny, chyba że, lub do momentu aż można będzie wykazać, że roszczenia w zakresie bezpieczeństwa nie są podważane przez to ograniczenie. Załóżmy na przykład, że test nie powiódł się, a w wyniku tego znaleziono w oprogramowaniu błąd, wtedy to ograniczenie (w zakresie poprawności oprogramowania) może być dowodem przeciwnym. Z drugiej strony, jeśli błąd tkwi w jakiejś funkcjonalności, która nie są związana z bezpieczeństwem, to jest prawdopodobne, że z punktu widzenia bezpieczeństwa, istnienie takiego błędu jest dopuszczalne, a więc to ograniczenie nie jest dowodem przeciwnym. Każdy członek projektu, który jest kompetentny w danym obszarze proceu, może rejestrować ograniczenia i oceniać ich wpływ w odniesieniu do zakresu tego procesu. Jednakże, dowód przeciwny jest całkowicie związany z bezpieczeństwem produktu i musi być oceniany przez właściwego specjalistę z zakresu bezpieczeństwa. W związku z tym ważne jest, żeby ograniczenia były dokładnie i przejrzyście rejestrowane w materiale dowodowym generowanym przez wszystkie procesy projektowe, i aby były zidentyfikowane w dokumentach podsumowujących proces, tak, aby mogły być poddane ocenie przez inżyniera ds. bezpieczeństwa.

Co zrobić, jeśli problem z testem oznaczał, że zamiast identyfikacji usterki w oprogramowaniu, test po prostu nie mógł być przeprowadzony? Tutaj problemem nie jest to, że o oprogramowaniu wiadomo jest, że jest nieprawidłowe: problemem jest to, że ponieważ test nie mógł być wykonany, nie ma dowodów na to, że oprogramowanie jest prawidłowe. Termin *brak zapewnienia* (assurance deficit) (Menon et al. 2010) stosuje się, gdy istnieje taka niepewność. Jednak, jak i w przypadku dowodów przeciwnych, ograniczenie w materiale dowodowym nie jest automatycznie deficytem zapewnienia/pewności/, gdy rozpatrujemy je w ogólnym kontekście kwestii bezpieczeństwa. Załóżmy, że weryfikacja oprogramowanie zostało przeprowadzona w zautomatyzowanym środowisku testowym, w którym nie można wykonać niektórych testów, tak, że wystepuje ograniczenie co do zakresu weryfikacji oprogramowania, jednak możliwe jest przeprowadzenie testu, który pozwala na osiągnięcie tych samych celów testowych w ogólnym środowisku systemu: w tym przypadku kwestię ograniczenia w testowaniu oprogramowania rozwiązuje się poprzez testowanie systemu, więc nie ma deficytu pewności. Braki pewności dotyczą ogólnej niepewności w sprawie bezpieczeństwa, więc tak jak z dowodami przeciwnymi, ocena tego, czy ograniczenia stanowią deficyty pewności, czy też nie, powinna być przeprowadzana przez właściwego specjalistę ds. bezpieczeństwa.

Zwalniając inżynierów ds. bezpieczeństwa z konieczności badania dużej ilości surowych ('nieobrobionych') dowodów niskiego poziomu, pozwala im się lepiej skoncentrować na kwestii bezpieczeństwa w kontekście ogólnym. W szczególności, zgodnie z Normą Obronną 00-56, poszukiwanie dowodów przeciwnych powinno być aktywne i powinno sięgać poza bezpośrednie środowisko danego projektu. Dodatkowo, widząc cały obraz przedstawiony przez materiał dowodowy, inżynierowie ds. bezpieczeństwa mogą być w lepszej pozycji do określenia "sprzecznych z intuicją" możliwości stwierdzonych przez Littlewooda i Wrighta (Littlewood i Wright 2007), gdzie bycie bardziej skutecznym w generowaniu dowodów może od czasu do czasu zmniejszać ogólną pewność siebie, czego przykładem jest to, że jeśli cały program testowy nie znajdzie żadnych błędów, to można podejrzewać, że system testowy jest nieskuteczny.

System zarządzania bezpieczeństwem powinien mieć konkretne cele do zarządzania identyfikacją, oceną i ograniczaniem deficytów pewności, oraz dowodów przeciwnych. Wyniki tego działania będą rejestrowane w raporcie dowodowym w kwestii bezpieczeństwa.

4.3 Raport dowodowy w kwestii bezpieczeństwa

Raport dowodowy w kwestii bezpieczeństwa jest ostatnim wymagalnym zadaniem z procesu zapewnienia. Ponieważ argument o bezpieczeństwie powinien być zaprojektowany tak, aby miał charakter abstrakcyjny, możliwe jest, aby jedna wersja argumentu o bezpieczeństwie objęła wiele instalacji oprogramowania, albo wiele realizacji w projektach implementowanych w systemie realizacji stopniowych. Jednakże, raport dowodowy w kwestii bezpieczeństwa będzie musiał zająć się konkretną wersją oprogramowania i konkretną instalacją. Raport dowodowy w kwestii bezpieczeństwa zidentyfikuje unikalny zestaw odpowiednich dowodów w kwestii bezpieczeństwa. Będzie musiał odnieść się do linii bazowej oprogramowania (która może być uwzględniona w standardowej dokumentacji, takiej jak uwagi do wydania oprogramowania), i będzie musiał odnieść się to do odpowiedniego zestawu dowodów bezpieczeństwa, w tym dowodów na poziomie systemu. Każda instalacja może mieć własny, niepowtarzalny dowód: specyficzne ograniczenie dla danego miejsca (site); wyjątkowa historia doświadczeń w terenie być może przy użyciu poprzednich wersji oprogramowania, oraz różne doświadczenia z eksploatacji (rozruchu).

Raport dowodowy w kwestii bezpieczeństwa jest wynikiem procesu oceny ograniczeń, deficytów ubezpieczeń i dowodów przeciwnych. Stanowi on podsumowanie procesu oceny i wynikającą z niego identyfikację deficytu ubezpieczeń i dowodów przeciwnych w kontekście ogólnym przypadku bezpieczeństwa. Będzie on również stanowił potwierdzenie pomyślnego funkcjonowania systemu zarządzania bezpieczeństwem.

Ponieważ ocenia on kompletny zbiór dowodów, jest w stanie ocenić, które części argumentu są poparte przekonywującymi dowodami, a które elementy są mniej przekonujące i dlatego pozostaje w nich śladowe ryzyko. Chociaż istnieje rozszerzenie do notacji GSN w celu określenia względnego udziału poszczególnych części argumentu, to nie wydaje się być stosowane w praktyce. Jest tak być może dlatego, że przydaje ono notacyjnej złożoności do tego, co i tak jest stanowi skomplikowane elementy analizy. Raport dowodowy w kwestii bezpieczeństwa wydaje się być bardziej odpowiednim miejscem, w którym da się zauważyć względne znaczenie różnych części argumentu, ponieważ można to określić w kontekście rzeczywiście dostarczonych dowodów. Jako ostatni rezultat procesu zapewniania bezpieczeństwa, raport dowodowy w kwestii bezpieczeństwa jest wydawany tym, którzy muszą podjąć decyzję o akceptacji lub odrzuceniu danego przypadku w kwestii bezpieczeństwa.

5 Wniosek

Artykuł ten nie jest studium teoretycznym, ale zamiast tego próbuje dać pragmatyczną wskazówkę w kwestiach zarządzania dużą ilość materiału dowodowego w obszarze zapewnienia bezpieczeństwa, gdyż w przypadku dużych projektów informatycznych wszelkie nieefektywności w tym obszarze będą w najlepszym razie kosztowne, a w najgorszym prowadzić będą do stworzenia słabego lub nieprawidłowego przypadku w zakresie bezpieczeństwa, lub też do poważnych opóźnień w dostarczaniu produktu do eksploatacji.

Kierownik projektu odpowiada za dostarczenie produktu, który jest zarówno bezpieczny, jak i postrzegany jako bezpieczny przez organ zawiadujący dowodami w zakresie zapewnienia bezpieczeństwa. Jednym z celów osadzonych w podejściu zaprezentowanym w tej pracy jest stworzenie takiej kultury, gdzie wszyscy członkowie zespołu projektowego są odpowiedzialni za dostarczenie dowodów na zapewnienie bezpieczeństwa w obszarach, za które odpowiadają. W takiej kulturze, inżynier ds. bezpieczeństwa nie działa w izolacji dokonując retrospektywnego przeglądu i oceny artefaktów projektu, ale jako partner pracuje prowadząc dialog z innymi ekspertami technicznymi w celu ustalenia procesów, które umożliwiają skuteczne zagwarantowanie bezpieczeństwa projektu jako całości.

Podejście oparło się na trzech zasadach przyswojonych z obszaru inżynierii oprogramowania: przesłanianie informacji; oddzielanie wymogów od konkretnej realizacji; oraz stopniową integrację. Argument o bezpieczeństwie powinien dotyczyć abstrakcyjnych (ogólnych) wymagań w zakresie dowodów, odraczając problem zajmowania się niepotrzebnymi szczegółami przy realizacji dowodów do czasu sporządzenia raportu dowodowego w kwestii bezpieczeństwa. Potrzebny jest środek identyfikowalności do zastosowania pomiędzy węzłami argumentu a ostatecznym materiałem dowodowym, być może przy użyciu relacyjnej bazy danych, która mogłaby również rejestrować status dowodów. Wreszcie, dowody należy oceniać sukcesywnie w miarę, jak są generowane, działając stopniowo - od szczegółowych nieprawidłowości specyficznych dla danego rodzaju dowodów, aby zrozumieć, jak mogą się one przyczyniać do wystąpienia ewentualnych deficytów zapewnień lub dowodów przeciwnych, a następnie określać odpowiednio takie

informacje w kontekście całości systemu, aby ocenić czy dowody dostarczają, lub też nie, zadowalający obraz kwestii bezpieczeństwa.

51

Proces wykazywania dowodów obejmuje systematyczne rejestrowanie i obiektywną ocenę dowodów, które generują, poprzez stosowanie właściwych osądów, dokładny ogólny obraz, w którym wszelkie problemy z dowodami są przedstawione przejrzyście po to, by dany przypadek bezpieczeństwa pokazywał dokładnie to, co zostało już osiągnięte, a co nadal pozostaje niesprawdzone.

Podziękowania Autor wyraża wdzięczność za dyskusje nt. argumentów o bezpieczeństwie i wnikliwy wgląd w SAEM (*safety argument evidence management*) przedstawiony przez dr Tima Kelly, University of York.

Literatura

Adelard (1998) ASCAD – Adelard safety case development manual Civil Aviation Authority (2010) CAP 670 ATS safety requirements European Commission (2008) Commission Regulation (EC) No 482/2008 Establishing a software safety assurance system to be implemented by air navigation service providers and amending annex II to regulation (EC) No 2096/2005 http://www.caa.co.uk/docs/952/ SESESARR%28482-2008%29.pdf. Accessed 12 September 2010

Hamilton V (2006) Criteria for safety evidence – goal-based standards require evidence based approaches. Safety Systems 16:1 September 2006. http://www.vivhamilton.co.uk/Papers/ SCEvCriteria.pdf. Accessed 12 September 2010

IEC (2000) ISO/IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems, Parts 1 to 7. International Electrotechnical Commission

Kelly T (1999) Arguing safety – a systematic approach to safety case management. PhD thesis, University of York YCST99/05

Littlewood B, Wright D (2007) The use of multi-legged arguments to increase confidence in safety claims for software-based systems: a study based on a BBN of an idealized example. IEEE Trans Softw Eng 33:347-365

Menon C, Hawkins R, McDermid J, Kelly T (2010) An overview of the SOBP for software in the context of DS 00-56 issue 4. In: Dale C, Anderson T (eds) Making systems safer. Sprin- ger-Verlag, London

Ministry of Defence (2007) Defence Standard 00-56 Issue 4: Safety management requirements for defence systems

Object Management Group (2010) Software assurance evidence metamodel (SAEM) Sysa/10- 02-01 http://www.omg.org/cgi-bin/doc?sysa/10-02-01. Accessed 23 March 2010

RTCA (1992) RTCA/DO-178B: Software considerations in airborne systems an equipment certi- fication. RTCA

xxxxxxxxxxxx