1.3 Analiza istniejących modeli zarządzania materiałem dowodowym

Jednym ze sposobów zarządzania materiałem dowodowym jest model oparty na wskazywaniu dowodów w ramach ukierunkowanych norm bezpieczeństwa oprogramowania. Przyjęcie takiego podejścia do zagadnienia zarządzania materiałem dowodowym wymaga dużej liczby dowodów bezpieczeństwa systemu generowanych w oparciu o wymogi projektowanego oprogramowania. Istotna jest w powyższym przypadku skuteczna ocena dowodów w celu optymalizacji ich ilości. Ukierunkowane normy bezpieczeństwa oprogramowania nie kwestionują roli argumentów ponieważ to one nadają sens dowodom jednak to dowody dają pewność bezpieczeństwa systemu. Ostatecznie wymagane jest aby wykazać że produkt jest akceptowalnie bezpieczny co jest możliwe tylko poprzez wskazanie bezsprzecznych na to dowodów.

Istotną kwestią w kontekście generowania dowodów jest wielkość projektu. Jeśli zakres prac jest niewielki dużo łatwiej zidentyfikować liczbę dowodów wystarczających do potwierdzenia zakładanej cechy systemu. Ryzyko niskiej efektywności a nawet bezużyteczności działań podejmowanych w zakresie identyfikacji i weryfikacji dowodów zwiększa się wraz z wydłużeniem w czasie procesów potrzebnych do wytworzenia oprogramowania. Efektem wzrostu takiego rodzaju ryzyka w projekcie jest zwiększenie kosztów i przekroczenie terminu wykonania o wysiłek który jest niezbędny do zagwarantowania właściwej oceny materiału dowodowego. Jeśli zbyt dużo czasu zajmie nam ocena zebranych dowodów niemal na pewno konieczne będzie okrojenie czasu potrzebnego przy innych czynnościach zmierzających do ograniczenia ryzyka. Konieczność efektywnego zarządzania materiałem dowodowym wymusza także kwestia uzyskania w określonym czasie akceptacji zdefiniowanych cech systemu przez organy nadzorujące proces wytwórczy.

Istotnym elementem analizy jest argument o bezpieczeństwie. Wymagane jest jego systematyczne kontrolowanie pod względem ważności w sposób manualny. Pomimo wprowadzenia standardów strukturyzujących m.in. GSN, CAE co pozowała na bardziej rygorystyczne analizowanie argumentu nieodzowna jest recenzja tego elementu wykonana przez ludzi. Przyjmuje się że argument musi być przedstawiony w sposób czytelny i zrozumiały. Obarczanie argumentu niepotrzebnymi szczegółami może skutkować że będzie on rozpatrywany w sposób fragmentaryczny z dużą dozą ryzyka pomijania istotnych interakcji zachodzących w jego wnętrzu. Skomplikowane określenie tego co jest argumentem może przyczynić się do podwyższenia trudności we właściwym zrozumieniu i w rezultacie błędnej interpretacji, ewentualnie zupełnego odrzucenia w trakcie weryfikacji. Rozwiązaniem w unikaniu podobnych sytuacji może być przyjęcie zasad abstrakcji oraz oddzielenia wymagań od realizacji tzn. argument musi zdefiniować wymagania dla różnych rodzajów dowodów ale jednocześnie pozostając niezależnym od szczegółów realizacji dowodów. Takie podejście umożliwia uzgodnienie argumentu bezpieczeństwa we wczesnym cyklu życia systemu. Zakończenie procedury potwierdzania wiarygodności wymaga przedstawienia sprawozdania dotyczącego dowodów śledzących procesy powiązane z tym argumentem.

Wspomniałem wcześniej, że częstym problemem obserwowanym w realizacji dużych projektów jest konieczność uzyskania akceptacji argumentu bezpieczeństwa ze strony wielu zainteresowanych stron m.in. organu nadzoru operacyjnego, integratora systemów, producenta oprogramowania i niezależnego eksperta w dziedzinie bezpieczeństwa. Istnieje zatem konieczność uzgodnienia argumentu na wczesnym etapie cyklu życia systemu w ramach planowania harmonogramu zarządzania bezpieczeństwem i tworzenia dokumentacji technicznej w tym planu rozwoju oprogramowania etapy oraz jego weryfikacji. Przeprowadzanie uzgodnień w zakresie argumentu jest możliwe na późniejszym etapie rozwoju projektu jednakże należy wówczas mieć na uwadze zwiększenie trudności w realizacji potrzeb w zakresie zapewnienia bezpieczeństwa. Stworzenie zwięzłego argumentu tj. ograniczonego do wymogów w zakresie dowodów które mają być wygenerowane i unikanie szczegółów ich realizacji powinno skrócić czas uzyskania akceptacji od wszystkich stron zainteresowanych projektem. Wymagania w zakresie dowodów mogą być określone jako cele rozwoju oprogramowania i jego weryfikacji. Szczegóły prezentacji tak wytworzonego materiału dowodowego zostaną określone w trakcie projektowania procesów oprogramowania. Przyjęcie tego podejścia jest zdecydowanie lepsze niż posiadanie zespołu ludzi zajmujących się bezpieczeństwem który narzuca szczegółową formę dowodów dla inżynierów oprogramowania ponieważ zmniejsza ryzyko wprowadzania zmian w ustalonych i „dojrzałych” procesach dostawcy oprogramowania.

Niestety nie da się całkowicie wykluczyć zmian argumentu bezpieczeństwa ponieważ w trakcie procesu wytwórczego mogą pojawić się nowe wymagania lub ograniczenia dotyczące bezpieczeństwa. Konieczność wprowadzenia zmian w zakresie definicji argumentu zachodzi także wówczas jeśli z różnych przyczyn zwiększy się liczba dowodów przeciwnych lub znacznej zmianie ulegną dotychczasowe procesy projektowo – wdrożeniowe. Dobrze zdefiniowany argument powinien dopuszczać możliwość absorbowania drobnych zmian przez szczegóły dostarczonych dowodów. Tylko istotne powinny stwarzać konieczność redefinicji całości lub niektórych fragmentów argumentu. Przykładem abstrahowania od zbędnych szczegółów które powodują że argument staje się odporny na drobne niespójności w materiale dowodowym jest sposób w jaki odnosi się on w kwestii bezpieczeństwa do ograniczeń dowodów i dowodów przeciwnych których zbiór zawiera dokument nazywany raportem dowodowym.

Argument powinien dotyczyć jedynie abstrakcyjnych wymagań w zakresie dowodów dlatego potrzebne są sposoby identyfikowania tych wymogów z konkretnymi realizacjami dowodów. Osiągniecie tego założenia ułatwia metoda w której argument identyfikuje symbole zastępcze w systemie zarządzania konfiguracją. Lepszy efekt powiązania argumentu z dowodami daje implementacja relacyjnej bazy danych. Zaletą bazy danych jest to że może ona przechowywać dodatkowe metadane np.: osoba odpowiedzialna za utworzenie dowodu, data utworzenia, ocena stanu kompletności dowodu oraz stopień asocjacji z argumentem. Organizacja The Object Management Group (OMG) opracowała schemat powiązania argumentu o bezpieczeństwie z dowodami przy użyciu metadanych tj. Software Assurance Evidence Metamodel (SAEM).

Kolejną kwestia którą należy poruszyć w ramach omawiania modelu opartym na wskazywaniu dowodów jest zarządzanie procesami tworzącymi dowody. Wspomniano już wcześniej o konieczności określenia argumentu bezpieczeństwa na możliwe wczesnym etapie tworzenia oprogramowania. Gwarantuje to że procesy które tworzą największą liczbę dowodów (szczegółowa specyfikacja oprogramowania, rozwój i weryfikacja oprogramowania, weryfikacja i walidacja systemu) mogą być projektowane w nastawieniu na wskazanie dowodów dających gwarancje bezpieczeństwa systemu. Charakteryzując argument bezpieczeństwie wskazałem że abstrakcyjne wymagania dla dowodów powinny być wyraźnie określone w dokumentach które określają procesy generujące te dowody np. odniesienia w argumencie o bezpieczeństwie do identyfikacji i oceny zagrożeń będą prawdopodobnie obsługiwane przez procesy inżynierii bezpieczeństwa, odniesienia do demonstracji zachowań oprogramowania przypuszczalnie będzie obsługiwane przez procesy testowania lub analizy oprogramowania. Określając wymagania dotyczące dowodów jako cele procesu, można zaprojektować dany proces tak aby generował dowody w wymaganej formie, zaś weryfikacja dopuszczalności dowodów może być normalną częścią weryfikacji procesu. Dodatkową korzyścią tego zastosowania jest to, że każdy członek projektu może zobaczyć, jak jego praca przyczynia się do produkcji bezpiecznego i gwarantującego pewną jakość produktu.

Przyjmując że mamy do czynienia dwoma rodzajami właściwości dowodów: te które mogą być obiektywnie ocenione oraz te które są przedmiotem oceny ekspertów można kształtować procesy tworzące dowody tak aby właściwości obiektywne uzyskiwać automatycznie. Przykład w inżynierii oprogramowania: środowisko programistyczne skonstruowane tak aby prawidłowo nazwane obiekty były przechowywane wraz z opisującymi je metadanymi w systemie zarządzania konfiguracją.