Programowanie Defensywne

Przegląd wybranych standardów
część druga

Arkadiusz Chrobot

Katedra Systemów Informatycznych

26 czerwca 2024

Plan

Wstęp

W pierwszej części wykładu kontynuujemy przegląd standardów bezpieczeństwa dla dziedzin zastosowania, biorąc pod uwagę sektor finansowy, w szczególności płatności kartami. Druga część zawiera opisy kilku mniej lub bardziej poważnych wypadków, gdzie zostało naruszone bezpieczeństwa związane z kwestią niezawodności (ang. *safety*), a których przyczyną były błędy w oprogramowaniu. Przedstawiono w niej także przykład systemu, który dzięki starannemu zaprojektowaniu od 46 lat prawidłowo funkcjonuje, mimo pracy w niesprzyjających warunkach.

Standardy dla sektora finansowego

Wstęp

Mechanizmy bezpieczeństwa dla instytucji finansowych (banki, firmy fintech, itp.) oparte są na zasadach księgowości, w szczególności na bilansie aktywów i pasywów. Z tego względu w finansowych systemach informatycznych najbardziej istotna jest *integralność* danych transakcji. Dlatego muszą one być wyposażone w wiarygodny system rejestrowania *danych audytowych*, pozwalających stwierdzić jakie operacje zostały przeprowadzone, przez kogo i kiedy. Dokładną strukturę tych danych mogą określać przepisy prawne obowiązujące w poszczególnych krajach, ale również może być ona opisana przez wewnętrzne standardy określonej instytucji finansowej.
Większość standardów bezpieczeństwa dla płatności kartami definiowana jest przez *Payment Card Industry Security Standard Council* ▸ PCI SSC.

Standardy dla sektora finansowego

PCI DSS

Za główny standard PCI dotyczący płatności kartą należy uznać *Data Security Standard* (PCI DSS) [1]. Obecnie obowiązuje wersja 4.0 tego standardu, która została opublikowana w marcu 2022. Jest to 360 stronicowy dokument zawierający wymagania techniczne i operacyjne dla środowisk, gdzie przetwarzane są dane posiadaczy kart, a także wytyczne dla ich implementacji i oceny. Część z tych wymagań, których łącznie jest 12 może dotyczyć twórców oprogramowania do obsługi płatności kartami. Każde z nich rozpisane jest na bardziej szczegółowe wymagania, których specyfikacje składają się z dwóch części, opisu wymagania i wytycznych pomagających to wymaganie spełnić. Opis z kolei może zawierać: tradycyjne metody implementacji i weryfikacji wymagania, zamierzony cel jego wprowadzenia i jego zakres zastosowania. W wytycznych mogą znaleźć się: objaśnienie celu wymagania, dobre praktyki, definicje, przykłady i dalsze informacje.

Standardy dla sektora finansowego

PCI DSS

Główne wymagania w tym standardzie to:

1. instalacja i utrzymanie mechanizmów bezpieczeństwa sieci,
2. zastosowanie bezpiecznej konfiguracji wszystkich komponentów systemu,
3. ochrona przechowywanych danych karty,
4. ochrona danych posiadaczy kart przy pomocy silnego szyfrowania podczas ich transmisji otwartymi, publicznymi sieciami,
5. ochrona wszystkich systemów i sieci przed złośliwym oprogramowaniem,
6. wytwarzanie i utrzymywanie bezpiecznego oprogramowania i bezpiecznych systemów,
7. ograniczenie dostępu do komponentów systemu i danych kart płatniczych według zasady wiedzy koniecznej,
8. identyfikacja użytkowników i uwierzytelnienie dostępu do komponentów systemu,

Standardy dla sektora finansowego

PCI DSS

9. ograniczenie fizycznego dostępu do danych posiadaczy kart,
10. rejestrowanie i monitorowanie wszystkich dostępów do komponentów systemu i danych posiadaczy kart,
11. regularne testowanie bezpieczeństwa systemów i sieci,
12. wsparcie bezpieczeństwa informacji politykami i programami organizacyjnymi.

Standardy dla sektora finansowego

PA-DSS

Jako uzupełnienie dla standardu PCI DSS został opracowany *Payment Applications Data Security Standard* (PA-DSS) [2], którego odbiorców stanowią producenci oprogramowania, jak również sprzętu w postaci terminali płatniczych. Podobnie jak PCI DSS, PA-DSS zawiera nie tylko wymagania, ale również wskazówki, jak je implementować oraz wytyczne dla audytorów. Ostatnią obowiązującą jego wersją była 3.0, opublikowana w listopadzie 2013 roku i wycofana z użycia w październiku 2022. **Standard PA-DSS nie jest już stosowany.** Zastąpił go zbiór norm PCI *Software Security Framework* (PCI SSF). Mimo, że PA-DSS już nie obowiązuje, to warto się zapoznać z zawartymi w nim wymaganiami, gdyż część z nich zostanie przeniesiona także do nowych norm. Jest ich 14, przy czym każde ma kilka podpunktów. Specyfikacja każdego wymagania składa się z trzech części: opisu wymagania, procedury testowej i wytycznych.

Standardy dla sektora finansowego

PA-DSS

1. zabronione jest przechowywanie (ang. *retain*) danych zapisywanych na karcie (ang. *full track data*), kodu lub wartości weryfikującej kartę (CAV2, CID, CVC2, CVV2) oraz PIN, zarówno w postaci jawnej, jak i zaszyfrowanej (ang. PIN *Block Data*),
2. ochrona przechowywanych danych właściciela karty,
3. zapewnienie środków uwierzytelniania,
4. rejestrowanie operacji aplikacji płatniczej,
5. opracowanie bezpiecznego wytwarzania aplikacji płatniczej,
6. ochrona transmisji bezprzewodowych,
7. testowanie podatności aplikacji płatniczych i zapewnianie jej aktualizacji,
8. wsparcie dla bezpiecznej transmisji w sieci,
9. zabronione jest przechowywanie danych właściciela karty na serwerze podłączonym do Internetu,

Standardy dla sektora finansowego

PA-DSS

10. wsparcie dla bezpiecznego dostępu zdalnego do aplikacji płatniczej,
11. szyfrowanie wrażliwych danych przesyłanych sieciami publicznymi,
12. szyfrowanie połączeń administracyjnych, niepochodzących z konsoli (czyli wykonywanych bezpośrednio przy użyciu klawiatur i monitora),
13. przygotowanie i utrzymanie przewodnika implementacji PA-DSS dla klientów, sprzedawców i integratorów,
14. wyznaczenie personelu odpowiedzialnego za zgodność z PA-DSS i prowadzenie szkoleń dla personelu, klientów, sprzedawców i integratorów.

Standardy dla sektora finansowego

PCI SSF

Zbiór norm PCI SSF [3] obejmuje standard bezpieczeństwa oprogramowania płatniczego, standard bezpiecznego wytwarzania oprogramowania płatniczego i wymagania dla firm prowadzących audyty w tych dwóch zakresach. Zawiera on wiele cech standardu PA-DSS, który zastąpił, ale celem jego twórców było przyspieszenie procedur oceniających, dostosowanie do ciągle powstających i ewoluujących usług finansowych (np. płatność kodem QR, płatność telefonem, zegarkiem), oraz nowych zagrożeń.

Standardy dla sektora finansowego

PCI SSF Secure Software Standard

Dokument PCI SSF *Secure Software Standard* [4] zawiera głównie opis procedury audytu, który teraz podzielono na dwie kategorie: audyt całkowity (ang. *full assessment*) i częściowy (po przyrostowej zmianie w oprogramowaniu, ang. *delta assessment*). Wytyczne zawarte w tej publikacji określają jakie elementy oprogramowania podlegają audytowi, ale nie określają wymagań[1]. Z procesu standaryzacji wyłączono oprogramowanie dla płatności opracowane i/lub używane wewnętrznie. Podlegają mu jedynie aplikacje tego typu stosowane powszechnie.

[1] Dokument jest w początkowej wersji, w kolejnych edycjach może się to zmienić.

Standardy dla sektora finansowego

PCI SSF Secure Software Life Cycle (Secure SLC) Standard

Dokument PCI SSF *Secure Software Life Cycle (Secure* SLC *Standard)* [5] to także opis procedur ewaluacji, ale dotyczących procesu wytwarzania i utrzymywania oprogramowania do płatności. W szczególności określa on zakres i częstotliwość ocen, wymaganą dokumentację, role i odpowiedzialności. Podobnie jak wcześniej opisywany dokument nie zawiera on wymagań.

Standardy dla sektora finansowego

PCI SSF Qualification Requirements for Accessors

Standard PCI SSF *Qualification Requirements for Accessors* jest (głównie) zbiorem wymagań, jakie musi spełniać firma posiadająca lub ubiegająca się o status audytora PCI SSF. Wymagania te podzielono na cztery kategorie:

1. biznesowe (legalność, niezależność, posiadanie ubezpieczenia, wniesienie opłat, podpisanie umów),
2. kompetencyjne (doświadczenie i świadczone usługi, doświadczenie i wiedza personelu, kodeks zawodowej odpowiedzialności),
3. administracyjne (osoba do kontaktów, weryfikacja życiorysu pracowników, wewnętrzne zapewnianie jakości, ochrona danych poufnych i osobowych, przechowywanie dowodów, procedury na wypadek incydentów, właściwe posługiwanie się statusem audytora),
4. kwalifikacyjne (coroczna ocena, kwalifikacje z zakres bezpieczeństwa oprogramowania).

Standardy dla sektora finansowego

Inne standardy PCI SSC

Warto dodać, że oprócz opisanych wcześniej dokumentów PCI SSC opublikował również standardy dla testów penetracyjnych i protokołu *3-D Secure*.

Kilka przepisów na katastrofę ...

Rakieta Ariane 5

W rakiecie Ariane 5 zastosowano oprogramowanie do sterowania z Ariane 4, która wyposażona była w słabsze silniki [6, 7]. Obie rakiety dysponowały dwoma rodzajami czujników. Jeden przekazywał tylko 16-bitowe liczby, a drugi mógł przekazywać albo 16 albo 64--bitowe wartości. W tym drugim przypadku konieczna była zatem alokacja pamięci. Konfiguracja tych czujników była inna w przypadku obu rakiet. Niestety jeden z czujników drugiego typu został skonfigurowany jako czujnik pierwszego typu. W trakcie lotu zaczął on podawać 64-bitowe wartości, które (częściowo) zostały potraktowane jako rozkazy. To spowodowało błędne działanie jednego z komponentów układu sterowania, który nadał raport o awarii, do centralnego procesora, łączem służącym do przesyłania danych nawigacyjnych. Skutkiem była niebezpieczna zmiana trajektorii, która groziła uderzeniem rakiety w obszary zamieszkałe. Naziemna obsługa zadecydowała o włączeniu mechanizmu samozniszczenia.

Kilka przepisów na katastrofę ...

F-22 Raptor

Sześć myśliwców F-22 Raptor lecących z Hawajów do bazy na Okinawie w lutym 2007 roku jednocześnie uległo awarii zaraz po przekroczeniu linii zmiany daty [6]. Wyłączyły się systemy nawigacji, kontroli paliwa oraz (częściowo) komunikacji i nie podjęły działania mimo kilkukrotnych prób restartu. Ostatecznie pilotom udało się wrócić na lotnisko lecąc za samolotem-cysterną. Siły Powietrzne Stanów Zjednoczonych (US Air Force) nie ujawniły jaka była dokładna przyczyna awarii, jedynie podały, że udało się ją usunąć w ciągu 48 godzin. Jej charakter wskazuje, że defekt mógł polegać na błędnej interpretacji daty przez oprogramowanie.

Kilka przepisów na katastrofę ...

Rakiety Patriot

W 1991 roku, podczas operacji Pustynna Burza, po raz pierwszy w historii użyto systemu Patriot do obrony baz amerykańskich przed atakami rakietowymi [6]. Pierwsza wersja tego systemu była zaprojektowana do użytku mobilnego, wiążącego się z częstym jego włączaniem i wyłączaniem. Jednakże w czasie wojny w Iraku były one stosowane stacjonarnie. Miało to wpływ na precyzję obliczania czasu, który był przechowywany jako 24-bitowa liczba zmiennoprzecinkowa. Jednostką tego czasu była $0,1$ sekundy. Wymagało to wykonania mnożenia przez tę właśnie liczbę, która w systemie binarnym jest nieskończonym ułamkiem okresowym. Zatem każde takie wyliczenie wprowadzało błąd na poziomie $0,000095\%$. W bazie znajdującej się w Arabii Saudyjskiej, koło miasta Dhahran, system Patriot był używany w trybie ciągłym przez około 100 godzin. To oznaczało, że jego wskazania czasu różnią się o około $\frac{1}{3}$ od czasu faktycznego. W związku z tym nie mógł on przechwycić rakiety Scud, która w tym czasie pokonuje około $0,5$ km.

Kilka przepisów na katastrofę ...

Mars Climate Orbiter

Wystrzelona w grudniu 1998 roku sonda Mars Climate Orbiter uległa zniszczeniu w atmosferze Marsa, zamiast wejść w jego orbitę [6]. W trakcie lotu na tę planetę wykorzystywała ona żyroskopy, aby ustabilizować swoją pozycję. Jednakże te urządzenia mają tendencję do przyspieszania swojego ruchu. Aby je spowolnić sonda wykonywała procedurę nazywaną „desaturacją momentu pędu" (ang. *angular momentum desaturation*), polegającą na włączeniu napędu na określony czas. Dane o tym jak długo był on włączony i na jaką moc ustawiony przesyłana była do NASA, gdzie program SM_FORCES, opracowany przez firmę Lockheed Martin przeliczał je i zapisywał w pliku na użytek zespołu odpowiedzialnego za nawigację. Programiści z Lockheed Martin użyli w obliczeniach funtów, czyli angielskich jednostek inżynierskich (poprawna nazwa systemu imperialnego), a pracownicy NASA zinterpretowali je jako Newtony, czyli jednostki siły z układu metrycznego. W rezultacie sonda znalazła się 57 km od powierzchni Marsa, zamiast 150–170.

Kilka przepisów na katastrofę ...

Knight Capital

W sierpniu 2012 roku Giełda Nowojorska wdrożyła Program Płynności Detalicznej (ang. *Retail Liquidity Program*), który pozwalał sprzedawcom, w określonych sytuacjach, oferować akcje detalicznym kupcom po trochę lepszych cenach [6]. Postanowiła skorzystać z tego firma Knight Capital, aktualizując swoje oprogramowanie do szybkiej sprzedaży (ang. *high-frequency trading*). Jednakże dokonując modyfikacji popsuli algorytm i program kupił akcje 154 spółek po cenach wyższych niż można je było sprzedać. W ciągu godziny straty firmy osiągnęły poziom $461,1$ miliona dolarów. Dokładnej przyczyny nie ujawniono, ale przypuszcza się, że zadziałał kod testujący, który nie powinien być aktywny, a spowodował to jeden błędny wiersz w programie. W konsekwencji firma Knight Capital musiała sprzedać 73% swoich udziałów konsorcjum spółek finansowych, aby ratować swoją sytuację.

Kilka przepisów na katastrofę ...

Algorytm wyceny portalu Amazon

Firma Amazon pozwala sprzedawcom określać cenę produktu oferowanego za pośrednictwem ich strony w sposób proceduralny [6]. Skorzystały z tego dwie firmy, które jako jedyne oferowały książkę do genetyki o tytule „The Making of a Fly". Przypuszczalnie jedna z nich określiła swoją strategię jako „określ moją cenę książki jako tańszą o $0,07\%$ od najniższej ceny konkurencji". Druga zaś zastosowała metodę „ustal moją cenę o 27% droższą od najtańszej oferowanej przez konkurencję". Swoista sytuacja hazardowa, spowodowana tym, że w sklepie Amazon zostały tylko dwa egzemplarze wspomnianej książki, doprowadziła do tego, że jeden z nich osiągnął cenę $23.698.655,93$ dolarów (bez kosztów wysyłki).

Kilka przepisów na katastrofę ...

Boeing 737 Max 8

Źle zaprojektowane oprogramowanie było bezpośrednią przyczyną wypadków samolotów Boeing 737 Max 8 należących do indonezyjskich i etiopskich linii lotniczych [8], w których zginęło łącznie ponad 350 pasażerów. Konstrukcja tego samolotu jest oparta na wcześniejszym modelu 737, ale zamontowano w niej większe silniki. Rozmiar tych silników wymagał innego ich mocowania w kadłubie samolotu, co z kolei spowodowało niestabilną charakterystykę jego lotu. Miał on tendencję do unoszenia przodu do góry w trakcie lotu, co prowadziło do niebezpiecznej sytuacji, nazywanej „przeciągnięciem". Tę wadę postanowiono wyeliminować przy pomocy oprogramowania MCAS (ang. *Maneuvering Characteristics Augmentation System*), którego zadaniem było „ściąganie" przodu samolotu w dół. Niestety, korzystało ono z tylko jednego czujnika kąta natarcia (ang. *Angle of Attack* (AOA)) i nie sprawdzało wiarygodności podawanych przez niego danych. Dodatkowo zostało zaprojektowane tak, aby ignorować działania pilotów starających się zmienić tor lotu maszyny.

Kilka przepisów na katastrofę ...

Boeing 737 Max 8

Boeing ukrył przed pilotami fakt istnienia oprogramowania MCAS, aby móc przedstawić nowy samolot jako niewielką modyfikację 737 i tym samym uniknąć kosztów i oczekiwania związanego z zatwierdzeniem nowego modelu przez FAA. Europejskiemu odpowiednikowi FAA przedstawiono MCAS jako niekrytyczny komponent samolotu.

...i jeden na sukces

Misja Voyager

Misja Voyager to dwie sondy kosmiczne wystrzelone w 1977 roku, które opuściły Układ Słoneczny i nadal nadają dane naukowe [9]. Zbudowano je zgodnie z trzema zasadami: niezawodność, nadmiarowość i rekonfigurowalność. Skorzystano ze sprawdzonych komponentów i zastosowano prototypowanie. Każdy istotny element został podwojony. Nawet sondy są dwie i lecą po trochę różnych trajektoriach. Ich pracę nadzorują trzy komputery. Pierwszy jest odpowiedzialny za pracę całości systemu. Jego podzespoły są podwójne i wykonane w technologi odpornej na promieniowanie radiacyjne. Pamięć tego komputera jest nieulotna i zawiera procedury należące do dwóch kategorii: niezmiennych i ładowanych zdalnie. Oprogramowanie tego komputera napisano w asemblerze lub języku Fortran. Jest on także wyposażony w autonomiczny moduł, który wykrywa usterki i próbuje je naprawić.

...i jeden na sukces

Misja Voyager

Podobnie jest zbudowany drugi komputer, odpowiedzialny za nawigację i orientację sondy w przestrzeni. Trzeci komputer zbiera i wysyła dane na Ziemię w czasie rzeczywistym. Aby transmisja była niezawodna zastosowano kod detekcyjno-korekcyjny. Komputer odpowiedzialny za dane jest także wyposażony w taśmę magnetyczną pełniącą rolę pamięci masowej. Jest ona używana wtedy, gdy sonda chwilowo nie może pozostać w kontakcie z Ziemią.

Literatura I

Gregory Travis. “How The Boeing 737 Max Disaster Looks To a Software Developer”. W: IEEE *Spectrum* (18 kw. 2019). URL: https://spectrum.ieee.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer.

PCI *Data Security Standard, Version 4.0*. URL: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf (term. wiz. 14. 06. 2023).

PCI *Payment Application Data Security Standard*. URL: https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf (term. wiz. 14. 06. 2023).

Literatura II

- PCI *Software Security Framework Provides a Moder Approach to Payment Software Security*. 2019. URL: https://listings.pcisecuritystandards.org/documents/SSF_At-a-Glance.pdf (term. wiz. 21. 06. 2023).
- PCI *Software Secuirty Framework Secure Software Standard*. URL: https://listings.pcisecuritystandards.org/documents/Secure-Software-Program-Guide-v1.pdf (term. wiz. 14. 06. 2023).
- PCI *Software Secuirty Framework Secure Software Life Cycle (Secure SLC) Standard*. URL: https://listings.pcisecuritystandards.org/documents/Secure-Software-Life-Cycle-(SLC)-Program-Guide-v1.pdf (term. wiz. 14. 06. 2023).
- Matt Parker. *What Happens When Maths Goes Wrong?* URL: https://youtu.be/6JwEYamjXpA?t=3745 (term. wiz. 19. 06. 2023).

Literatura III

Aaron Cummings. *Uptime 15,364 days - The Computers of Voyager*. URL: https://www.thestrangeloop.com/2019/uptime-15-364-days---the-computers-of-voyager.html (term. wiz. 19. 06. 2023).

Matt Parker. *Humble Pi: A Comedy of Maths Errors*. United Kingdom: Pinguine Random House UK, 2019.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!