PROJEKT SYSTEMU WSPOMAGAJĄCEGO NADZÓR I ZARZĄDZANIE FLOTĄ AUTOBUSÓW

W artykule przedstawiono projekt systemu informatycznego wspomagającego zarządzanie flotą autobusów. Utrzymanie wysokiej pozycji na rynku jest dla firm transportowych priorytetem. Nie jest jednak możliwe bez świadczenia wysokiej jakości usług, sprawnej komunikacji, redukcji kosztów i zapewnienia wysokiego poziomu bezpieczeństwa. Wszystkie te obszary muszą być wspomagane przez system informatyczny. W artykule przedstawiono wymagania jakie musi spełnić taki system oraz zaproponowano jego koncepcję. Szczególny nacisk położono na aspekt bezpieczeństwa i niezawodności systemu.

WSTĘP

Na rynku usług przewozu pasażerów istnieje silna konkurencja. Rozwój firmy w tak trudnych warunkach wymaga zapewnienia usług o jak najwyższej jakości przy zachowaniu niskiej ceny. Nie mniej istotnym aspektem jest również zapewnienie pasażerom bezpieczeństwa. Spełnienie powyższych wymagań nie jest możliwe bez sprawnego systemu pozwalającego na kompleksowe zarządzanie flotą autobusów. Istniejące na rynku systemy przeznaczone do tego celu posiadają zaimplementowany jedynie fragment niezbędnych funkcjonalności. Jednym z dedykowanych systemów zarządzania flotą autobusów jest Flota-Online. Oferuje on kontrolę stanu paliwa, monitorowanie parametrów jazdy kierowcy, wysyłanie informacji o punktach docelowych, komunikację z kierowcą, lokalizację pojazdów oraz pobieranie danych z tachografów [3]. Innym rozwiązaniem pozwalającym na monitorowanie floty jest SAS Flota Premium [9]. System ten jest dedykowany do zarządzania dowolną flotą pojazdów. Oznacza to, że posiada uniwersalną funkcjonalność obejmującą takie aspekty jak: lokalizację GPS, informowanie o prędkości i kierunku poruszania się, informacje o stylu jazdy kierowcy, otwarciu ładowni i jej zamknięciu, temperaturze ładowni, poziomie paliwa czy danych odczytywanych z szyny CAN pojazdu. Mimo deklaracji producenta o dostosowaniu systemu do obsługi floty autobusów funkcjonalność bardziej się wpisuje w potrzeby firm transportowych przewożących ładunki. O wiele lepiej dostosowany do monitorowania floty autobusów jest system Navifleet. Oprócz kontroli pozycji GPS, odczytu danych z komputera pokładowego i kontroli stylu jazdy kierowcy oferuje kontrolę przewozu klientów. Pozwala na weryfikację czy pasażer został odebrany z umówionego miejsca i czy został dostarczony tam gdzie zostało to wskazane. Dodatkowo oferowana jest funkcjonalność kontroli czasu odebrania oraz dostarczenia pasażerów na miejsce [8]. Dedykowany system dla floty autobusów ma również firma Volvo. Jednak jej system również ogranicza się do monitorowania lokalizacji pojazdu, jego stanu technicznego oraz zdarzeń a także stylu jazdy kierowcy. System ten oferuje rozbudowany moduł raportowania ukierunkowany na kontrolę wydajności oraz kosztów transportu [10]. Podobną funkcjonalność oferują inne konkurencyjne systemy takie jak Daimler FleetBoard [5] czy WebFleet [4]. Widoczny jest więc brak systemu, który integrował by wszystkie funkcje niezbędne w zarządzaniu flotą autobusów. W niniejszym artykule podjęto próbę przeprowadzenia analizy potrzeb i zaproponowania koncepcji systemu będą-

cego w stanie w pełni wspierać firmy świadczące usługi transportu pasażerskiego.

1. ANALIZA POTRZEB RYNKU

Potrzeby rynkowe należy rozpatrywać z dwóch różnych perspektyw:

- pasażera, który jest zainteresowany ceną oraz jakością usługi a także pakietem dodatkowych funkcjonalności ułatwiających dostęp do informacji oraz ułatwiających załatwienie formalności,
- przewoźnika – będącego firmą zainteresowaną maksymalizacją zysków oraz zdobywaniem coraz lepszej pozycji rynkowej,
- kierowcy, który bezpośrednio odpowiada za realizację transportu.

Jakość usług zazwyczaj jest oceniana bezpośrednio przez klienta na podstawie doświadczeń zawiązanych z korzystaniem z usługi. W przypadku przewozów pasażerskich najczęściej brane są pod uwagę takie aspekty jak:

- wygoda i komfort,
- solidność,
- dostępność,
- dostosowanie do potrzeb klientów,
- kompetencja i uprzejmość personelu,
- zrozumienie wymagań klienta,
- wiarygodność,
- bezpieczeństwo,
- informacja,
- niezawodność,
- wartości dodane [1, 2].

Uzyskanie wysokiej jakości oferowanych usług wymaga ciągłego podnoszenia jakości wszystkich operacji wchodzących w zakres usługi lub ją wspomagających [2]. Badanie preferencji podróżnych przeprowadzone przez przedsiębiorstwo SBB w Stuttgarcie wykazało, że najważniejsze dla pasażerów są:

- zapewnienie połączeń,
- punktualność,
- częstotliwość kursów,
- bezpieczeństwo,
- czystość,
- uprzejmość i kompetencja personelu,
- dostęp do informacji,
- łatwość zakupu biletów [2].

Utrzymanie wysokiej jakości usług, zwłaszcza w aspekcie wymienionych priorytetów pasażerów wymaga utrzymania ścisłej kontroli przez zarządcę floty. Od jakości usług i cen przewozów zależała będzie liczba klientów a co za tym idzie zyski firmy. Jednak ważnym aspektem jest tu również istnienie konkurencji. Każde przedsiębiorstwo nastawione jest na zysk i zdobycie jak największego udziału w rynku. Zauważyć też należy, że każdy z przewoźników będzie potrzebował takich samych środków do wykonania usługi. A mianowicie: pojazdu, którym przewiezie pasażera i kierowcy, który poprowadzi pojazd. Dodatkowo niezbędne jest zaplecze w postaci usługi sprzedaży biletów i planowania tras wraz z częstotliwością kursów oraz usługi serwisowej pozwalającej na utrzymanie właściwego stanu technicznego floty.

Analiza struktury kosztów ponoszonych przez przewoźników wskazuje dwa istotne czynniki wpływające na kształtowanie kosztów: zakup paliwa oraz koszty wynagrodzeń. W sumie stanowią one około 50% kosztów ponoszonych przez każdą firmę transportową. Jako, że silna konkurencja wymusza stosowanie zbliżonych cen przez wszystkich przewoźników to zysk firmy zależał będzie w głównej mierze od poziomu kosztów. Istotna jest więc ich redukcja tam gdzie to możliwe oraz optymalizacja procesów pozwalająca na zwiększenie efektywności transportu. Możliwe jest to jedynie przy utrzymaniu doskonałego przepływu informacji oraz zastosowaniu systemu kontroli transportu działającego w czasie rzeczywistym.

2. WYMAGANIA FUNKCJONALNE SYSTEMU INFORMACYJNEGO

System informatyczny jest narzędziem pozwalającym na swobodny przepływ informacji oraz świadczenie usług na odległość bez udziału ludzi. Dzięki temu pozwala na optymalizację procesów, ich kontrolę oraz redukcję kosztów poprzez zmniejszenie pracochłonności. Rozpatrując potrzeby przedsiębiorstwa możemy wyszczególnić następujące wymagania funkcjonalne:

- monitoring poziomu paliwa w czasie rzeczywistym pozwalający na wykrywanie wszelkich prób kradzieży paliwa oraz na porównywanie danych o poziomie paliwa z informacją o spalaniu pochodzącą z silnika pojazdu,
- lokalizacja pojazdu pozwalająca monitorować jego ruch w celu określenia zgodności z rozkładem jazdy oraz w przypadku prób kradzieży czy innych problemów wymagających zlokalizowania pojazdu,
- monitorowanie stylu jazdy kierowcy w trakcie jazdy z funkcją informowania go o popełnionych błędach oraz zaleceniami dotyczącymi poprawy stylu jazdy pozwalającymi na zredukowanie spalania oraz poprawę komfortu jazdy pasażerów a także jako czynnik motywujący pozwalający na premiowanie kierowców osiągających doskonałe wyniki,
- monitorowanie danych diagnostycznych pojazdu pobieranych z szyny CAN w celu wykrycia nieprawidłowości w pracy oraz odpowiednio wczesnego zaplanowania wizyty pojazdu w serwisie,
- bieżąca weryfikacja stopnia bezpieczeństwa pojazdu oraz pasażerów poprzez odczyt danych z czujników umieszczonych w pojeździe, takich jak nadmierne przechylenie, gwałtowne hamowanie i przyspieszanie, wciśnięcie przycisku alarmowego przez kierowcę czy jazda z otwartymi drzwiami lub z niesprawnymi podzespołami,
- monitorowanie czasu pracy kierowcy, pozwalające na uniknięcie kar za przekroczenie ustawowego czasu pracy,
- definiowanie rozkładów jazdy i przypisywanie do poszczególnych kursów kierowców i autobusów,

- sprzedaż biletów poprzez stronę WWW dostępną również na urządzeniu mobilne oraz poprzez interfejs kierowcy umożliwiający zakup biletu bezpośrednio w autobusie,
- ewidencjonowanie wolnych i zajętych miejsc na poszczególnych odcinkach trasy w celu umożliwienia sprzedaży biletów na wybrane odcinki,
- informowanie pasażerów o rozkładzie jazdy autobusów,
- dostarczanie pasażerom informacji o przewidywanym czasie dojazdu autobusu do wybranego przystanku oraz o liczbie wolnych miejsc możliwych do zakupu na wybranym odcinku,
- rejestrowanie obrazu i dźwięku z wnętrza autobusu i zapisywanie go na nośniku znajdującym się w pojeździe,
- strumieniowanie obrazu i dźwięku z autobusu do systemu informatycznego na żądanie operatora,
- informowanie kierowcy o fakcie „wypadnięcia” z rozkładu jazdy oraz przesyłanie mu danych trasy na urządzenie mobilne,
- wyszukiwanie połączeń dla pasażerów podróżujących z przesiadkami,
- raportowanie liczby pasażerów podróżujących na określonych trasach w podziale na godziny dnia i dni tygodnia oraz w wybranych przedziałach czasu w sposób pozwalający zoptymalizować dobór wielkości autobusów i częstotliwości ich kursowania na poszczególnych trasach,
- raportowanie przemieszczania się pasażerów z punktu do punktu w podziale na godziny dnia w celu ustalania nowych tras dostosowanych do potrzeb licznych grup pasażerów,
- planowanie przerw serwisowych i przeglądów technicznych pojazdów,
- planowanie grafika pracy kierowców z funkcją optymalizacji wykorzystania czasu pracy kierowców,
- możliwość dołączenia interfejsów firm trzecich, świadczących usługi komplementarne, takich jak wyszukiwarki noclegów, wyszukiwarki sklepów, restauracji, aptek i innych punktów usługowych.

3. KONCEPCJA TOPOLOGII SYSTEMU

Zrealizowanie rozwiązania pozwalającego na kompleksową obsługę floty autobusów wymaga odpowiedniej topologii systemu, gwarantującej bezpieczeństwo oraz wydajność systemu. Schemat proponowanej topologii został zaprezentowany na rysunku 1.

Przedstawiony na rysunku 1 system składa się z wielu elementów. Podstawowym elementem dostarczającym informacji i kontrolującym stan pojazdu jest układ elektroniczny wyposażony w różnego rodzaju czujniki, GPS, kompas, żyroskop oraz moduł łączności GSM. Układ ten został nazwany centralką pojazdu. Dodatkowo do zbierania danych używany jest telefon kierowcy. Gromadzi on niezależne dane o położeniu, które pozwalają na zweryfikowanie poprawności lokalizacji pojazdu przesłanej przez centralkę pojazdu. Dane zebrane przez centralkę i telefony kierowców są przesyłane do serwera zbierającego dane z pojazdów. Rolą tego serwera jest niezawodne odebranie przesyłanych danych oraz zapisanie ich w bazie danych, która została umieszczona na klastrze serwerów. Klaster jest grupą komputerów posiadających tę samą funkcjonalność. Serwery wchodzące w skład klastra wymieniają się danymi w taki sposób by każdy z nich posiadał aktualną kopię bazy danych. Dzięki temu w przypadku awarii jednego z nich pozostałe przejmują jego funkcje i baza danych działa bez przerw a dane nie są tracone. Klaster pełni więc funkcję niezawodnościową. Dodatkowo, każdy z serwerów wchodzących w skład klastra może niezależnie odpowiadać na żądania innych maszyn i dostarczać im danych. Dzięki temu zwiększa się wydajność bazy danych.

Rys. 1. Schemat topologii systemu

Kłaster bazodanowy stanowi źródło informacji dla dwóch niezależnych serwerów WWW. Pierwszy z nich jest publicznie dostępny, przeznaczony do obsługi klientów, którzy poprzez przeglądarkę mogą korzystać z oferowanych usług informacyjnych oraz dokonać zakupu biletów. Ze względu na nieograniczoną dostępność tego serwera jest on szczególnie narażony na ataki przychodzące z Internetu. Z tego też powodu został on umieszczony za firewalliem, który ogranicza zagrożenie poprzez filtrowanie ruchu sieciowego. Nie jest jednak możliwe doskonałe zabezpieczenie tego serwera. Dlatego też w strukturze systemu został przewidziany drugi serwer z którego korzystają pracownicy firmy transportowej. Dostarcza on interfejsu, poprzez który pracownicy wykonują swoją pracę.

4. ANALIZA BEZPIECZEŃSTWA POŁĄCZEŃ

System monitorowania floty jest niewątpliwie strukturą w znacznym stopniu narażoną na ataki. Unieruchomienie takiego systemu pozbawi firmę możliwości nadzoru nad transportem i pojazdami oraz znacząco obniży jakość świadczonych usług a nawet może prowadzić do paraliżu firmy transportowej ze względu na utratę możliwości sprzedaży biletów i określenia liczby wolnych oraz wykupionych miejsc. Istotne jest więc skuteczne zabezpieczenie systemu przed atakami. W proponowanym rozwiązaniu komunikacja pomiędzy poszczególnymi elementami systemu odbywa się za pomocą wirtualnej sieci prywatnej (VPN), która przesyła wszystkie dane w postaci zaszyfrowanej w sposób uniemożliwiający podłączenie się osób postronnych. Dzięki temu dane są zabezpieczone przed podsłuchem a elementy systemu nie są narażone na ataki

z zewnątrz. Dostęp do nich mogą uzyskać tylko inne elementy znajdujące się wewnątrz tego samego VPN. Komunikacja pomiędzy centralkami pojazdów, telefonami kierowców oraz punktem dostępowym (BTS) operatora telefonii komórkowej jest również zabezpieczona poprzez APN operatora, który zapewnia szyfrowanie przesyłanych danych. Na schemacie przedstawionym na rysunku 1 wszystkie bezpieczne połączenia szyfrowane zostały oznaczone kolorem zielonym.

Najbardziej zagrożonym elementem systemu jest serwer WWW świadczący usługi dla klientów. Zagrożenie wynika z udostępnienia go w sieci Internet, gdzie jest narażony na różnego rodzaju ataki. Zagrożenie to można zminimalizować poprzez ciągłą aktualizację oprogramowania serwera, udostępnienie na zewnątrz jedynie usługi WWW oraz umieszczenie serwera za firewalliem, który będzie analizował połączenia przychodzące do serwera. Na schemacie przedstawionym na rysunku 1 połączenia z sieci publicznej oznaczono kolorem czerwonym. Kolorem żółtym oznaczono fragment sieci znajdującej się za firewalliem.

5. AUTENTYKACJA

Potwierdzenie tożsamości drugiej strony komunikacji jest niewątpliwie problemem w każdym systemie informatycznym. Istotne jest bowiem określenie czy nadawca danych jest tym, za którego się podaje. W przeciwnym wypadku istniała by możliwość podpięcia do systemu fałszywego źródła danych, które będzie wysyłało nieprawdziwe dane.

Konieczna jest również weryfikacja odbiorców danych pozwalająca uniknąć sytuacji, w których atakujący uzyskuje chronione dane z systemu informatycznego.

W omawianym projekcie zastosowano infrastrukturę klucza publicznego (PKI) do uwierzytelniania i autentykacji urządzeń w systemie. Każde z nich zostało wyposażone w unikatowy klucz prywatny. Dzięki temu każde z urządzeń może potwierdzić swoją tożsamość podpisując dane swoim kluczem prywatnym. Weryfikacja tożsamości komunikującego się urządzenia odbywa się poprzez pobranie certyfikatu tegoż urządzenia z urzędu certyfikacji (CA) i zweryfikowanie poprawności złożonego podpisu cyfrowego. Inicjacja komunikacji w proponowanym systemie będzie zawierała element uwierzytelnienia obydwu stron komunikacji i będzie przebiegała według schematu przedstawionego na rysunku 2. Każde z urządzeń będzie korzystało z własnego klucza prywatnego do złożenia podpisu potwierdzającego jego tożsamość. Weryfikacja podpisu będzie się odbywała poprzez jego weryfikację na podstawie certyfikatu klucza publicznego pobranego z serwera CA. W trakcie uwierzytelniania odbiorca wygeneruje klucz sesji, który prześle w postaci zaszyfrowanej do nadawcy. Klucz sesji będzie kluczem kryptograficznego algorytmu symetrycznego, zapewniającego dużą szybkość szyfrowania i deszyfrowania.

Aspektem, którego nie można pominąć w tej analizie są koszty proponowanego rozwiązania. W przypadku zakupu certyfikatów na rynku koszt certyfikatu dla jednego urządzenia wyniesie ponad 100zł rocznie. W przypadku dużej liczby urządzeń koszt ten będzie znaczący. Jednak możliwe jest uniknięcie tego wydatku poprzez uruchomienie własnego CA. Będzie ono odpowiednie do zabezpieczenia komunikacji pomiędzy urządzeniami wchodzącymi w skład systemu. CA możliwe jest do uruchomienia jako usługa działająca na serwerze zbierającym dane z pojazdów. Pełną funkcjonalność CA oferuje darmowa biblioteka OpenSSL [6], z której funkcjonalności możemy skorzystać w systemie Linux [7].

Jedynym komercyjnym certyfikatem, który będzie konieczny do zastosowania w proponowanym systemie jest certyfikat serwera WWW świadczącego usługi dla klientów. Serwer ten musi być

wyposażony w certyfikat rozpoznawany przez wszystkie urządzenia, z których będą korzystali klienci firmy. Pozwoli to na autentykację serwera oraz na stosowanie protokołu HTTPS do transmisji pomiędzy klientami a serwerem. Protokół ten zapewnia szyfrowanie wszystkich przesyłanych danych co pozwala na zabezpieczenie przed podsłuchem oraz uniemożliwia przejęcie sesji przez atakującego.

Rys. 2. Schemat procesu autoryzacji

PODSUMOWANIE

Przedstawiony projekt systemu wspomagającego zarządzanie flotą autobusów zawiera kompleksowe rozwiązanie pozwalające na usprawnienie zarządzania flotą. Najważniejszym aspektem jest kompleksowość rozwiązania, której brakuje systemom dostępnym na rynku. Ze względu na kluczową rolę systemu szczególny nacisk położono na kwestie bezpieczeństwa systemu. Dzięki zastosowaniu VPN zabezpieczono system przed atakami pochodzącymi z Internetu. Wyjątkiem jest tu serwer WWW świadczący usługi dla klientów, który ze względu na specyfikę swojego działania musi być dostępny z dowolnego urządzenia w sieci Internet. Jednak nawet skuteczne unieruchomienie tego serwera nie wpływa na pracę pozostałej części systemu, umożliwiając sprawne działanie firmy pomimo ataku na system informatyczny.

Odporność na awarie sprzętu uzyskano poprzez zastosowanie klastra serwerów. Zapewnia on ciągłość dostępu do danych nawet pomimo awarii jednego z serwerów wchodzących w jego skład. W przypadku pozostałych serwerów zrezygnowano z zastosowania klastrów ze względu na wysokie koszty tego rozwiązania. Zaprojektowano je jako maszyny o zwiększonej odporności na uszkodzenia sprzętu. Odporność tą uzyskuje się poprzez użycie serwera, który

ma zduplikowaną większość elementów – znajdziemy w nim dwa zasilacze, co najmniej dwa procesory, wiele kości pamięci RAM oraz macierze dyskowe RAID 5 zapewniające ciągłą pracę nawet w przypadku awarii jednego z dysków serwera.

Wykorzystanie kryptografii klucza publicznego pozwoliło na bezproblemową autentykację wszystkich urządzeń wchodzących w skład systemu. Dzięki zastosowaniu własnego urzędu certyfikacji możliwe było uniknięcie kosztów wyposażenia urządzeń w klucze prywatne.

BIBLIOGRAFIA

1. J. Toruński, Jakość usług transportowych w przewozach pasażerskich, Zeszyty Naukowe AKADEMII PODLASKIEJ w SIEDL-CACH NR 82 Seria: Administracja i Zarządzanie, 2009
2. A. Mężyk, S. Zamkowska, Podnoszenie jakości usług w przewozach pasażerskich, Technika Transportu Szynowego nr.3, s. 21-27, 2004
3. Autobusy i autokary, <http://flota-online.pl/oferta-monitoringu-pojazdow/monitoring-gps-autobusow-autokarow>, dostęp elektroniczny dn. 26.03.2018r.
4. Czym jest zarządzanie flotą pojazdów?, https://telematics.tomtom.com/pl_pl/webfleet/fleet-management/, dostęp elektroniczny dn. 26.03.2018r.
5. Daimler: Nowa darmowa aplikacja dla zarządzania flotą, <http://www.eprzewoznik.pl/technika-telematyka/daimler-nowa-darmowa-aplikacja-dla-zarzadzania-flota/>, dostęp elektroniczny dn. 26.03.2018r.
6. OpenSSL Cryptography and SSL/TLS Toolkit, <https://www.openssl.org/>, dostęp elektroniczny dn. 27.03.2018r.
7. openssl(1) - Linux man page, <https://linux.die.net/man/1/openssl>, dostęp elektroniczny dn. 27.03.2018r.
8. Przewozy pasażerskie, <https://www.navifleet.pl/zastosowania-dla-firm/przewozy-pasazerskie.html>, dostęp elektroniczny dn. 26.03.2018r.
9. SAS Flota Premium, <http://www.sasgps.pl/flota-premium>, dostęp elektroniczny dn. 26.03.2018r.
10. Zarządzanie flotą kontrola online w czasie rzeczywistym, <http://www.volvobuses.pl/pl-pl/our-offering/services/fleet-management.html>, dostęp elektroniczny dn. 26.03.2018r.

A project of a system supporting bus fleet management and supervision

Paper discusses a project of a system to support bus fleet management. Such a system is necessary to keep high position on market. A lack of complex solution available made us to design a new safe system from scratch. The paper analyses the transport firms needs and defines system functionality necessary to support efficiently a fleet of buses. The design is focused on IT system security and reliability.

Autorzy:

mgr **Marta Dziuba-Kozieł** – Politechnika Lubelska, Wydział Elektrotechniki i Informatyki

dr inż. **Grzegorz Kozieł** – Politechnika Lubelska, Wydział Elektrotechniki i Informatyki, Instytut Informatyki

JEL: L63 DOI: 10.24136/atest.2018.223

Data zgłoszenia: 2018.05.28 Data akceptacji: 2018.06.15