Analiza ruchu urządzeń IoT

Wprowadzenie

Internet Rzeczy (IoT) to rewolucyjna technologia, która łączy przedmioty codziennego użytku z internetem, umożliwiając im gromadzenie, wymianę i przetwarzanie danych. Urządzenia IoT, od inteligentnych termostatów i przenośnych monitorów aktywności fizycznej po czujniki przemysłowe, umożliwiają bezproblemową komunikację, automatyzację i podejmowanie decyzji w oparciu o dane w różnych branżach. Urządzenia IoT stwarzają wiele wyzwań i zagrożeń dla bezpieczeństwa, prywatności i niezawodności. Urządzenia IoT są często narażone na ataki, takie jak podsłuch, podszywanie się pod inne urządzenia, manipulacje, odmowa usługi (DAS) lub infekcja złośliwym oprogramowaniem. Urządzenia IoT mogą również ujawniać poufne lub osobiste informacje, takie jak lokalizacja, aktywność, preferencje lub stan zdrowia. Urządzenia IoT mogą również działać nieprawidłowo lub zachowywać się nieprzewidywalnie z powodu błędów oprogramowania, awarii sprzętu lub problemów z siecią. Dlatego ważne jest, aby rejestrować i analizować ruch (pakiety danych) urządzeń IoT. Możemy uzyskać wgląd w wzorce komunikacji i protokoły używane przez te urządzenia, analizując ruch urządzeń IoT. Możemy również wykrywać i zapobiegać potencjalnym zagrożeniom lub anomaliom, które mogą wpływać na wydajność lub bezpieczeństwo tych urządzeń. W tym rozdziale przedstawimy koncepcję i charakterystykę urządzeń IoT oraz ich protokołów komunikacyjnych. Omówimy również przypadki użycia sniffingu sieciowego urządzeń IoT w różnych scenariuszach. Następnie zaprezentujemy działanie narzędzi i technik służących do sniffingu i analizy ruchu z urządzeń IoT za pomocą Wiresharka, popularnego narzędzia do analizy sieci. Pokażemy również kilka przykładów interpretacji i wizualizacji danych o ruchu urządzeń IoT za pomocą Wiresharka. Pod koniec tego rozdziału będziesz w stanie rejestrować i analizować ruch urządzeń IoT za pomocą Wiresharka oraz zrozumieć korzyści i wyzwania z tym związane.

Cele

Celem jest przedstawienie koncepcji i charakterystyki urządzeń IoT oraz ich protokołów komunikacyjnych. Ma on również na celu zaprezentowanie przypadków użycia sniffingu sieciowego urządzeń IoT w różnych domenach i scenariuszach. Ponadto ma on na celu nauczenie czytelników, jak korzystać z Wiresharka, narzędzia do analizy sieci, do rejestrowania i analizowania ruchu urządzeń IoT. Ponadto ma on pomóc czytelnikom zrozumieć, jak interpretować i wizualizować dane dotyczące ruchu urządzeń IoT za pomocą Wiresharka. Wreszcie, ma on na celu umożliwienie czytelnikom docenienia korzyści i wyzwań związanych z sniffingiem i analizą ruchu urządzeń IoT pod kątem bezpieczeństwa, prywatności i niezawodności.

Wprowadzenie do IoT

IoT (Internet Rzeczy) stał się rewolucyjną technologią, która łączy świat fizyczny z cyfrowym, umożliwiając urządzeniom komunikację, gromadzenie i wymianę danych oraz wykonywanie inteligentnych działań. Urządzenia IoT, znane również jako urządzenia inteligentne lub urządzenia połączone, stanowią rdzeń tej rewolucyjnej koncepcji.

Czym są urządzenia IoT?

Urządzenia IoT to obiekty fizyczne wyposażone w czujniki, oprogramowanie i łączność sieciową, które umożliwiają im interakcję z otoczeniem i innymi urządzeniami. Urządzenia te mogą obejmować zarówno proste przedmioty codziennego użytku, takie jak termostaty, żarówki i zamki do drzwi, jak i bardziej złożone systemy, takie jak maszyny przemysłowe, pojazdy i monitory medyczne. Są one zaprojektowane do wykrywania, przetwarzania i przesyłania danych do pamięci masowej w chmurze

lub innych urządzeń w celu analizy i podjęcia działań. Kluczową cechą urządzeń IoT jest możliwość łączenia się z Internetem, co umożliwia im komunikację między sobą i z użytkownikami. Wykorzystują one różne technologie komunikacyjne, takie jak Wi-Fi, Bluetooth, sieci komórkowe i połączenia satelitarne, do nawiązywania łączności. Ta łączność umożliwia zdalne sterowanie, monitorowanie i zarządzanie urządzeniami IoT, zapewniając wygodę, automatyzację i wydajność w różnych aspektach naszego życia. Urządzenia IoT wykorzystują czujniki do gromadzenia danych o otoczeniu. Czujniki te mogą mierzyć temperaturę, wilgotność, światło, ruch, ciśnienie i inne parametry. Przekształcają te informacje fizyczne w dane cyfrowe, które są następnie przetwarzane i analizowane lokalnie lub w chmurze. Urządzenia IoT mogą również zawierać siłowniki, które umożliwiają im wykonywanie działań na podstawie otrzymywanych danych. Na przykład inteligentny termostat może regulować temperaturę w pomieszczeniu na podstawie sygnału z czujników temperatury. Dane gromadzone przez urządzenia IoT mogą mieć istotne znaczenie w różnych zastosowaniach. W inteligentnych domach urządzenia IoT mogą automatyzować zadania, takie jak sterowanie oświetleniem, monitorowanie zużycia energii czy zarządzanie systemami bezpieczeństwa. W przemyśle urządzenia IoT mogą optymalizować procesy produkcyjne, śledzić zapasy lub monitorować wydajność sprzętu w celu zwiększenia wydajności i produktywności. W służbie zdrowia urządzenia IoT mogą monitorować parametry życiowe pacjentów, umożliwiać zdalne monitorowanie pacjentów, a nawet wspomagać zabiegi chirurgiczne. Jednak powszechne stosowanie urządzeń IoT budzi obawy dotyczące prywatności, bezpieczeństwa i zarządzania danymi. Ponieważ urządzenia te gromadzą i przesyłają poufne dane, kluczowe jest wdrożenie solidnych środków bezpieczeństwa w celu ochrony przed nieautoryzowanym dostępem i potencjalnymi naruszeniami.

Główne komponenty ekosystemu IoT

Ekosystem IoT to sieć połączonych ze sobą urządzeń, systemów i platform, które umożliwiają gromadzenie, przesyłanie, przetwarzanie i podejmowanie działań z wykorzystaniem Internetu lub innych sieci. Ekosystem IoT może składać się z różnych komponentów, w zależności od rodzaju i przeznaczenia systemu IoT, ale niektóre z głównych komponentów to:

Czujniki i siłowniki: Urządzenia te mogą wykrywać, mierzyć lub kontrolować parametry fizyczne, takie jak temperatura, wilgotność, ruch, światło, temperatura. Mogą również generować, przetwarzać i przesyłać dane do kolejnego komponentu. Czujniki i siłowniki łączą świat fizyczny z cyfrowym.

Łączność: Ten komponent umożliwia komunikację i przesyłanie danych między czujnikami, siłownikami i innymi komponentami ekosystemu IoT. Może wykorzystywać różne technologie i protokoły, takie jak Ethernet, Wi-Fi, Bluetooth, sieć komórkowa, RFID, NFC, MQTT itp. Może również wykorzystywać bramki lub urządzenia brzegowe do gromadzenia i przesyłania danych do kolejnego komponentu.

Przetwarzanie danych: Ten komponent przechowuje i analizuje dane zebrane przez czujniki i siłowniki. Może wykorzystywać środowiska lub serwery chmury obliczeniowej do zarządzania danymi, ich przetwarzania, wizualizacji i analizy. Może również zapewniać interfejsy i aplikacje umożliwiające użytkownikom dostęp do danych i urządzeń IoT oraz interakcję z nimi.

Akcja danych: Ten komponent uruchamia akcje lub odpowiedzi na podstawie analizy danych lub instrukcji. Akcje te mogą być wykonywane przez same czujniki i siłowniki, takie jak regulacja temperatury, oświetlenia lub zabezpieczeń domu, lub przez inne systemy lub użytkowników, takie jak wysyłanie alertów, powiadomień lub rekomendacji.

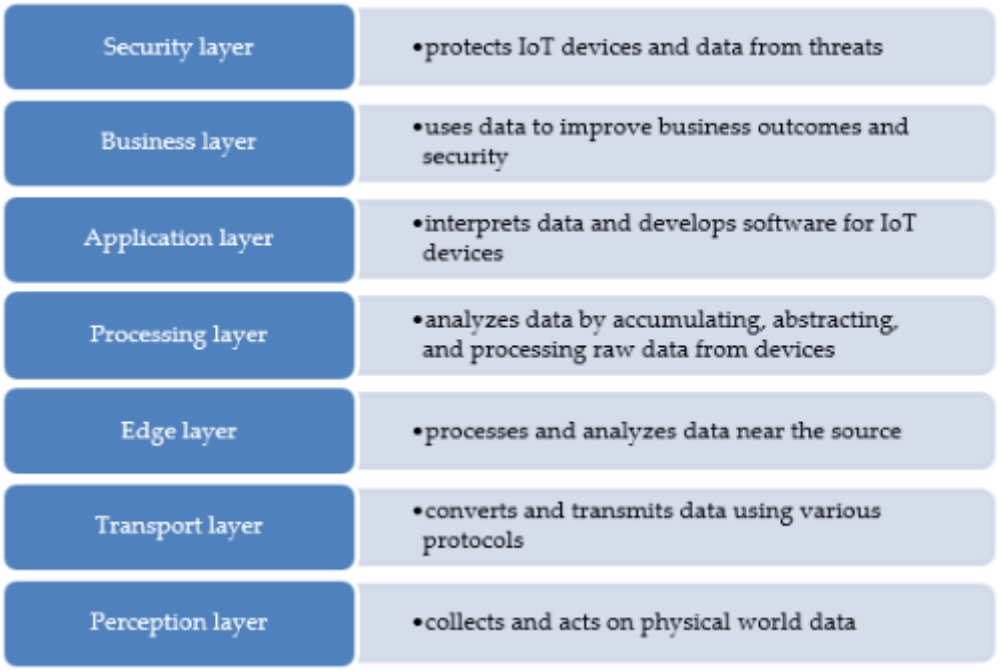
Interfejs użytkownika: Ten komponent umożliwia użytkownikowi interakcję z ekosystemem IoT. Może to być aplikacja internetowa lub mobilna, która zapewnia użytkownikom informacje, sterowanie,

informacje zwrotne lub opcje personalizacji. Może to być również interfejs głosowy lub oparty na gestach, który umożliwia naturalną interakcję z urządzeniami IoT.

Bezpieczeństwo: Ten komponent zapewnia ochronę i prywatność danych i urządzeń IoT. Może wykorzystywać różne metody i technologie, aby zapobiegać nieautoryzowanemu dostępowi, modyfikacji lub ujawnieniu danych za pomocą technik kryptograficznych; do uwierzytelniania i autoryzacji użytkowników i urządzeń; oraz w celu zapewnienia zgodności z przepisami i normami.

Architektura Internetu Rzeczy (IoT)

Architektura Internetu Rzeczy (IoT) odnosi się do sposobu organizacji różnych części systemu IoT i ich wzajemnego współdziałania. System IoT to system, który łączy różne elementy, takie jak urządzenia, maszyny czy obiekty, z internetem i umożliwia im komunikację oraz wymianę danych. Dane te mogą być wykorzystywane do dostarczania użytkownikom użytecznych informacji lub usług, a także do poprawy wydajności systemu. Architektura Internetu Rzeczy składa się z sześciu warstw:



Omówmy szczegółowo każdą warstwę:

Warstwa percepcji

Warstwa percepcji to część architektury systemu IoT, która oddziałuje ze światem fizycznym. Składa się z różnych komponentów, takich jak czujniki, kamery, siłowniki i inne urządzenia, które gromadzą dane i wykonują działania. Na przykład czujnik IoT może pomóc w kontroli jakości na linii produkcyjnej samochodów. Może sprawdzić, czy robot prawidłowo zmontował skrzynkę bezpieczników, analizując kolory poszczególnych bezpieczników. Jeśli robot umieścił bezpiecznik w niewłaściwym gnieździe, czujnik może to wykryć i zaalarmować system.

Warstwa transportu

W architekturze systemu IoT warstwa transportu odgrywa kluczową rolę w ułatwianiu transmisji danych z wielu urządzeń, takich jak czujniki, kamery i siłowniki, do scentralizowanego centrum danych zlokalizowanego lokalnie lub w chmurze. Aby to osiągnąć, bramy IoT służą do konwersji przychodzących danych analogowych z urządzeń na format cyfrowy. Po zdigitalizowaniu danych brama

wykorzystuje różne protokoły przesyłania danych (DTP) do przesyłania danych do centrum danych. Wybór odpowiedniego protokołu przesyłania danych zależy od kilku istotnych czynników. Należą do nich: ilość i rodzaj przesyłanych danych, pożądana prędkość i interwał transmisji, niezawodność połączenia sieciowego, zużycie energii podczas transmisji danych, wymagania dotyczące bezpieczeństwa danych i sieci oraz potrzeba komunikacji między urządzeniami brzegowymi w systemie IoT. Dostępnych jest kilka zróżnicowanych i powszechnie stosowanych protokołów IoT do przesyłania danych. Niektóre z tych protokołów to:

Message Queue Telemetry Transport (MQTT): Pierwotnie zaprojektowany przez IBM, MQTT to lekki protokół wykorzystujący schematy interakcji publikuj/subskrybuj. W protokole Message Queuing Telemetry Transport (MQTT) model interakcji publikuj/subskrybuj jest podstawowym wzorcem komunikacji. Jest to wzorzec przesyłania wiadomości, który umożliwia klientom wymianę wiadomości za pomocą tematów. Stał się najszerzej stosowanym protokołem w domenie IoT ze względu na swój charakter open source i przydatność dla urządzeń zlokalizowanych w odległych obszarach o ograniczonej łączności z internetem.

Modbus: Modbus to protokół komunikacji danych pierwotnie zaprojektowany z myślą o programowalnych sterownikach logicznych (PLC) produkowanych przez Modicon (obecnie Schneider Electric). Jest często używany do łączenia komputera nadzorującego ze zdalnymi terminalami (RTU) w systemach IoT, zgodnie z modelem SCADA (Supervisory Control And Data Acquisition).

Advanced Message Queuing Protocol (AMQP): AMQP został opracowany głównie przez JPMorgan Chase do przesyłania danych w sektorze usług finansowych. Jest znany ze swojego wbudowanego frameworka bezpieczeństwa, który wykorzystuje komponenty, takie jak Transport Layer Security (TLS) i Simple Authentication And Security Layer (SASL).

Sieć procesowa (PROFINET): PROFINET to protokół kompatybilny z Ethernetem, opracowany i obsługiwany przez PROFIBUS i PROFINET International (PI), niemiecką społeczność zajmującą się automatyzacją. Zyskał on szerokie zastosowanie w systemach automatyki przemysłowej, które wymagają komunikacji między wieloma urządzeniami brzegowymi, maszynami i systemami oprogramowania.

Magistrala CAN (Controller Area Network Magistrala): Zaprojektowana pierwotnie przez firmę Bosch dla przemysłu motoryzacyjnego, magistrala CAN umożliwia bezpośrednią komunikację między różnymi urządzeniami i czujnikami w pojeździe, eliminując potrzebę pośredniczącego komputera. Została zaadaptowana do różnych aplikacji dwukierunkowej komunikacji urządzeń, w tym między innymi do statków morskich, sprzętu budowlanego, systemów sterowania oświetleniem, sterowania windami i schodami ruchomymi.

Ethernet dla technologii automatyki sterowania (EtherCAT): EtherCAT to protokół oparty na sieci Ethernet, przeznaczony dla systemów wymagających aktualizacji danych w czasie rzeczywistym, opracowany przez Beckhoff, niemiecką firmę zajmującą się automatyzacją przemysłową. Jest szeroko stosowany jako protokół bramy IoT i jest obsługiwany przez EtherCAT Technology Group (ETG), grupę przemysłową zrzeszającą tysiące organizacji członkowskich.

Oprócz tych protokołów dostępnych jest kilka innych protokołów przesyłania danych (DTP), takich jak Constrained Application Protocol (CoAP) i Data Distribution Service (DDS). Protokoły te są szeroko stosowane w przemysłowych i nieprzemysłowych aplikacjach IoT, w tym w oświetleniu domowym, systemach bezpieczeństwa i inteligentnych urządzeniach medycznych.

Warstwa brzegowa

Wraz ze wzrostem skali sieci IoT, opóźnienia stają się poważnym wyzwaniem dla wydajności ze względu na przeciążenie spowodowane przez liczne urządzenia łączące się z centralnym węzłem. Aby rozwiązać ten problem, przetwarzanie brzegowe jest stosowane w warstwie brzegowej architektury systemu IoT, umożliwiając przetwarzanie i analizę danych jak najbliżej źródła danych.

Jedną z kluczowych cech wspólnych wszystkich urządzeń brzegowych IoT jest ich zdolność do przesyłania wykrytych danych w postaci pakietów danych do węzłów w celu dalszego przetwarzania. Niektóre zaawansowane urządzenia brzegowe są nawet zaprogramowane do podejmowania działań, takich jak zatrzymanie określonego procesu lub zainicjowanie środków kontroli uszkodzeń, w przypadku wykrycia poważnej anomalii. Urządzenia brzegowe IoT są zazwyczaj projektowane z myślą o bezproblemowej współpracy z urządzeniami różnych producentów. Ta interoperacyjność ma kluczowe znaczenie dla powszechnego stosowania urządzeń brzegowych w rozległych systemach IoT. Wstępne przetwarzanie danych to szybko rozwijająca się funkcja systemów IoT, która oferuje szereg korzyści. Umożliwia ona szybkie wykrywanie i rozwiązywanie problemów, jednocześnie redukując koszty związane z przesyłaniem dużych wolumenów danych. Istnieją jednak pewne wady, które należy wziąć pod uwagę. Wykorzystanie zaawansowanych procesorów do wstępnego przetwarzania danych może zwiększyć koszty instalacji i utrzymania warstwy sieciowej. Ponadto istnieje potencjalne ryzyko naruszenia bezpieczeństwa danych zdalnych. Co więcej, istnieje możliwość odfiltrowania cennych spostrzeżeń z danych urządzeń IoT, zanim będą mogły zostać poddane dalszemu przetwarzaniu. Zalety i wady: Wstępne przetwarzanie danych w bramach IoT. Oto zalety i wady włączenia wstępnego przetwarzania danych na poziomie sieci w bramach IoT. Zalety są następujące:

Szybkie generowanie cennych spostrzeżeń

Zmniejszenie kosztów związanych z transmisją danych

Możliwość szybkiego rozwiązywania lokalnych problemów

Wady to:

Wysokie koszty związane z procesorami brzegowymi

Obawy o bezpieczeństwo danych zdalnych

Możliwa utrata cennych spostrzeżeń

Warstwa przetwarzania

Warstwa przetwarzania, znana również jako warstwa pośrednicząca, jest kluczowym elementem architektury systemu IoT. Wykorzystuje ona przetwarzanie w chmurze i wiele połączonych komputerów w celu zwiększenia wydajności obliczeniowej, pamięci masowej, sieci i bezpieczeństwa. W architekturze systemu IoT warstwa przetwarzania jest niezbędna do analizy danych wejściowych w celu generowania cennych spostrzeżeń, prognoz i terminowych ostrzeżeń. Ponieważ system IoT przetwarza ogromne ilości danych generowanych przez liczne urządzenia brzegowe zlokalizowane na różnych krawędziach sieci, warstwa pośrednicząca wykorzystuje trzyetapowy proces przygotowywania tych danych dla warstwy aplikacji, który jest opisany w następujący sposób:

1. Akumulacja danych: Na tym etapie warstwa pośrednicząca precyzyjnie identyfikuje i przypisuje różne typy danych do odpowiednich pamięci masowych. Dane nieustrukturyzowane, takie jak strumienie audio i wideo oraz obrazy, zazwyczaj wymagają więcej miejsca na dysku i są przechowywane w jeziorach danych. Jezioro danych to scentralizowane repozytorium, które umożliwia przechowywanie ogromnych ilości danych ustrukturyzowanych i nieustrukturyzowanych w dowolnej

skali. Z kolei dane ustrukturyzowane, takie jak pomiary, rekordy i sygnały, są bardziej kompaktowe i przechowywane w repozytoriach danych.

2. Abstrakcja danych: Ten etap obejmuje agregację danych z wielu źródeł i zapewnienie ich konwersji do formatu zrozumiałego dla oprogramowania w warstwie aplikacji. Abstrakcja danych pomaga w standaryzacji danych i zapewnieniu ich zgodności z wymaganiami oprogramowania.

3. Analiza danych: Na tym etapie do zgromadzonych i wyabstrahowanych danych stosuje się algorytmy uczenia maszynowego (ML) lub głębokiego uczenia. Algorytmy te zostały zaprojektowane specjalnie w celu identyfikacji wzorców w dużych i pozornie losowych zbiorach danych. Analizując dane, warstwa przetwarzania może wyodrębnić istotne informacje, zidentyfikować trendy i sformułować prognozy, które przyczyniają się do ogólnej funkcjonalności i inteligencji systemu IoT.

Warstwa aplikacji

Warstwa aplikacji w architekturze systemu IoT odgrywa kluczową rolę w dekodowaniu znaczących wzorców w ogromnych ilościach danych generowanych przez urządzenia IoT. Polega ona na analizie tych danych i przekształcaniu ich w zwięzłe i zrozumiałe podsumowania, takie jak wykresy i tabele, łatwe do zinterpretowania przez ludzi. Warstwa aplikacji obejmuje również tworzenie programów i oprogramowania do sterowania urządzeniami, monitorowania i sterowania procesami. Aplikacje te umożliwiają efektywne zarządzanie i obsługę urządzeń IoT, zapewniając płynne działanie i efektywne wykorzystanie technologii IoT w różnych branżach.

Warstwa biznesowa

Warstwa biznesowa w architekturze systemu IoT odnosi się do etapu, na którym wzorce zidentyfikowane na poziomie aplikacji są analizowane i wykorzystywane do wydobywania cennych spostrzeżeń biznesowych. Spostrzeżenia te mogą następnie zostać wykorzystane do przewidywania przyszłych trendów i podejmowania świadomych decyzji operacyjnych, które poprawiają różne aspekty funkcjonalności biznesowej, takie jak wydajność, bezpieczeństwo, opłacalność i doświadczenie klienta. Wszystkie te korzystne rezultaty można osiągnąć, koncentrując się na warstwie biznesowej w architekturze systemu IoT. Oto kluczowe aspekty warstwy biznesowej w IoT:

Wykorzystanie danych: Warstwa biznesowa odpowiada za definiowanie sposobu wykorzystania danych zebranych z urządzeń IoT do osiągnięcia określonych celów biznesowych. Obejmuje to określenie, które dane są istotne, w jaki sposób są przetwarzane oraz jakie wnioski lub działania można z nich wyciągnąć.

Reguły i logika biznesowa: Definiuje reguły, logikę i algorytmy wykorzystywane do przetwarzania danych IoT. Może na przykład określać progi wyzwalania alertów, reguły automatyzacji dla urządzeń IoT lub algorytmy konserwacji predykcyjnej.

Integracja: Rozwiązania IoT często wymagają integracji z istniejącymi systemami biznesowymi, takimi jak oprogramowanie do planowania zasobów przedsiębiorstwa (ERP), systemy zarządzania relacjami z klientami (CRM) lub narzędzia do zarządzania łańcuchem dostaw. Warstwa biznesowa obsługuje te

integracje, aby zapewnić płynne działanie.

Bezpieczeństwo i zgodność: Zapewnienie prywatności danych, bezpieczeństwa i zgodności z przepisami jest kluczowym obowiązkiem warstwy biznesowej. Zapewnia ona kontrolę dostępu, szyfrowanie i zgodność z odpowiednimi standardami i przepisami branżowymi.

Warstwa bezpieczeństwa

Warstwa bezpieczeństwa w architekturze systemu IoT jest kluczowym elementem, który zaspokaja krytyczną potrzebę ochrony urządzeń i danych IoT. Co ciekawe, chociaż bezpieczeństwo ma ogromne znaczenie, stanowi ono poważne wyzwanie dla architektury IoT i samych urządzeń. Warstwę bezpieczeństwa można ogólnie podzielić na trzy kluczowe aspekty:

Bezpieczeństwo sprzętu: Ten aspekt obejmuje zabezpieczenie samych fizycznych urządzeń IoT. Koncentruje się na wdrażaniu środków chroniących te punkty końcowe przed atakami złośliwego oprogramowania i nieautoryzowanym dostępem. W celu zapewnienia integralności, poufności i dostępności urządzeń IoT stosowane są solidne protokoły i mechanizmy bezpieczeństwa. Bezpieczeństwo w chmurze: Biorąc pod uwagę, że znaczna ilość danych IoT jest przetwarzana i przechowywana w chmurze, kluczowe jest priorytetowe traktowanie bezpieczeństwa chmury. Wiąże się to z wdrożeniem solidnych środków bezpieczeństwa zapobiegających wyciekom danych, nieautoryzowanemu dostępowi i naruszeniom poufnych informacji. Szyfrowanie, kontrola dostępu oraz system wykrywania i reagowania na punkty końcowe (EDR) są powszechnie stosowane w celu zwiększenia bezpieczeństwa chmury w architekturze systemu IoT. Bezpieczeństwo połączeń: Aspekt bezpieczeństwa połączeń w warstwie bezpieczeństwa IoT kładzie nacisk na ochronę danych przesyłanych przez sieci. Jest to osiągane przede wszystkim poprzez techniki szyfrowania, które zapewniają poufność i integralność przesyłanych danych. Protokół Transport Layer Security (TLS) jest powszechnie uważany za punkt odniesienia w zabezpieczaniu połączeń IoT. Jest on powszechnie używany do ustanawiania bezpiecznych kanałów komunikacyjnych między urządzeniami IoT a innymi komponentami.

Dzięki uwzględnieniu tych trzech aspektów w warstwie bezpieczeństwa architektury systemu IoT organizacje mogą ograniczyć ryzyko związane z wdrażaniem IoT, poprawić ogólny poziom bezpieczeństwa oraz chronić prywatność i integralność urządzeń i danych IoT.

Jak działa IoT

Podstawowe działanie IoT można opisać w następujących krokach:

Gromadzenie danych: Urządzenia IoT posiadają czujniki lub urządzenia, które mogą wykrywać, mierzyć lub kontrolować parametry fizyczne, takie jak temperatura, wilgotność, ruch, światło itp. Mogą one również generować, przetwarzać i przesyłać dane do następnego etapu.

Transmisja danych: Urządzenia IoT wykorzystują różne technologie i protokoły do łączenia się i komunikacji ze sobą oraz z Internetem lub innymi sieciami. Mogą korzystać z połączeń przewodowych lub bezprzewodowych, takich jak Ethernet, Wi-Fi, Bluetooth, sieć komórkowa, RFID, NFC, MQTT itp. Mogą również korzystać z bram sieciowych lub urządzeń brzegowych do gromadzenia i przesyłania danych do następnego etapu.

Przetwarzanie danych: Dane IoT są przechowywane i analizowane w środowiskach chmury obliczeniowej lub na serwerach. Wykorzystują one różne platformy i usługi do zarządzania danymi, przetwarzania, wizualizacji i analizy.

Mogą również zapewniać interfejsy i aplikacje umożliwiające użytkownikom dostęp do danych i urządzeń IoT oraz interakcję z nimi.

Akcja na danych: Dane IoT mogą wyzwalać działania lub reakcje na podstawie analizy lub instrukcji. Działania te mogą być wykonywane przez urządzenia IoT (np. regulacja temperatury, oświetlenia lub zabezpieczeń domu) lub przez inne systemy lub użytkowników (np. wysyłanie alertów, powiadomień lub zaleceń).

Działanie lub architektura Internetu Rzeczy (IoT) może się różnić w zależności od rodzaju i przeznaczenia systemu IoT. Na przykład, konsumencki IoT . Działanie lub architektura Internetu Rzeczy (IoT) może się różnić w zależności od rodzaju i przeznaczenia systemu. Na przykład, konsumencki IoT odnosi się do urządzeń osobistych i przenośnych, które łączą się z internetem; przemysłowy IoT odnosi się do połączonych ze sobą urządzeń w sektorze przemysłowym; a inteligentne miasta odnoszą się do systemów IoT, które usprawniają usługi miejskie. Jednak kluczowa koncepcja ich działania jest podobna: wykorzystują one urządzenia IoT do gromadzenia i przesyłania danych ze świata fizycznego do cyfrowego i odwrotnie.

Korzyści z Internetu Rzeczy (IoT)

Urządzenia IoT mogą przynieść wiele korzyści osobom prywatnym, firmom i społeczeństwu. Oto niektóre z głównych korzyści:

Kontrola i automatyzacja: Urządzenia IoT umożliwiają użytkownikom sterowanie i automatyzację różnych zadań i procesów, takich jak regulacja temperatury, oświetlenia lub bezpieczeństwa w domu, a także planowanie dostaw towarów i usług.

Dostęp do informacji w czasie rzeczywistym: Urządzenia IoT mogą dostarczać użytkownikom dane i analizy w czasie rzeczywistym dotyczące ich otoczenia, zdrowia, aktywności lub wydajności, co może pomóc im w podejmowaniu lepszych decyzji i poprawie jakości życia.

Rozwijające się firmy: Urządzenia IoT mogą tworzyć nowe możliwości dla innowacji, przedsiębiorczości i tworzenia wartości, ponieważ mogą wspierać nowe produkty, usługi, modele biznesowe i rynki.

Zaawansowane gromadzenie danych: Urządzenia IoT mogą gromadzić duże ilości danych z różnych źródeł i kontekstów, które można analizować i wykorzystywać do różnych celów, takich jak optymalizacja operacji, poprawa jakości obsługi klienta, opracowywanie nowych rozwiązań lub generowanie przychodów.

Zwiększona produktywność i efektywność: Urządzenia IoT mogą pomóc firmom zwiększyć produktywność i efektywność poprzez automatyzację zadań, redukcję błędów, oszczędność czasu, poprawę jakości oraz optymalizację zasobów i aktywów.

Łatwość komunikacji: Urządzenia IoT mogą ułatwiać komunikację i współpracę między użytkownikami, urządzeniami, systemami i organizacjami poprzez wykorzystanie różnych protokołów i standardów do wymiany danych i informacji.

Efektywność kosztowa: Urządzenia IoT mogą pomóc użytkownikom oszczędzać pieniądze poprzez redukcję kosztów operacyjnych, zużycia energii, wytwarzania odpadów lub wydatków na konserwację.

Inteligentne miasta: Urządzenia IoT mogą pomóc w tworzeniu inteligentnych miast, które są bardziej przyjazne dla życia, zrównoważone, odporne i sprzyjające włączeniu społecznemu, poprzez poprawę usług miejskich, takich jak transport, energia, woda, gospodarka odpadami, opieka zdrowotna, edukacja czy bezpieczeństwo publiczne.

Poprawa bezpieczeństwa pracy: Urządzenia IoT mogą pomóc w poprawie bezpieczeństwa pracy poprzez monitorowanie niebezpiecznych środowisk, wykrywanie potencjalnych zagrożeń lub wypadków, ostrzeganie pracowników lub władz lub zapewnianie środków ochronnych.

Ograniczenia Internetu Rzeczy (IoT)

IoT ma również pewne ograniczenia, o których musimy pamiętać. Oto niektóre z nich:

Bezpieczeństwo i prywatność: Urządzenia IoT gromadzą i wysyłają wiele danych o nas i naszym otoczeniu, które mogą zostać zhakowane lub ujawnione przez osoby o złych zamiarach. Nie mamy również pełnej kontroli nad tym, jak nasze dane są wykorzystywane lub udostępniane innym osobom, które mają do nich dostęp.

Zależność i niezawodność: Urządzenia IoT są zależne od połączenia internetowego i sieciowego, które może być niestabilne lub niedostępne. Awaria lub przerwa w działaniu systemu może powodować problemy lub niedogodności dla nas i naszych urządzeń.

Standaryzacja i interoperacyjność: Urządzenia IoT wykorzystują różne technologie i standardy, co może powodować ich niekompatybilność lub utrudniać współpracę ze sobą. Potrzebujemy wspólnych zasad i regulacji, aby zapewnić jakość i spójność urządzeń i usług IoT.

Złożoność i konserwacja: Urządzenia IoT wymagają większych zasobów i infrastruktury do obsługi ich funkcjonowania i zarządzania. Im więcej urządzeń posiadamy, tym bardziej skomplikowana i wymagająca jest ich konserwacja, aktualizacja i integracja.

Urządzenia IoT: Przypadki użycia sniffingu sieciowego

Oto przykłady urządzeń IoT lub scenariuszy, w których sniffing sieciowy może być pomocny lub pouczający:

Czujniki: Czujniki to jeden z najstarszych i najbardziej rozpowszechnionych typów urządzeń IoT, używanych zarówno przez ludzi, jak i organizacje. Mogą mierzyć różne czynniki środowiskowe, takie jak temperatura, wilgotność, światło, ruch itp. Sniffing sieciowy może pomóc w monitorowaniu danych z czujników, rozwiązywaniu problemów z łącznością lub wykrywaniu anomalii lub włamań.

Inteligentne urządzenia domowe: Inteligentne urządzenia domowe to interaktywne urządzenia elektroniczne, które wykorzystują połączenia bezprzewodowe do rozumienia instrukcji użytkownika i wykonywania różnych zadań, takich jak regulacja termostatu, zamykanie drzwi lub odtwarzanie muzyki. Sniffing sieciowy może pomóc w analizie protokołów komunikacyjnych i formatów danych używanych przez te urządzenia, a także w ocenie ich zagrożeń dla bezpieczeństwa i prywatności.

Technologie noszone: Technologie noszone to urządzenia IoT, które można nosić na ciele, takie jak smartwatche, trackery fitness lub słuchawki douszne. Mogą łączyć się z innymi urządzeniami (takimi jak smartfony) lub internetem w celu udostępniania danych lub dostępu do usług. Podsłuchiwanie sieci może pomóc zrozumieć, w jaki sposób te urządzenia gromadzą i przesyłają dane osobowe, takie jak wskaźniki zdrowia, lokalizacja lub preferencje.

Osobiste urządzenia medyczne: Osobiste urządzenia medyczne to urządzenia IoT, które mogą monitorować lub leczyć różne schorzenia, takie jak rozruszniki serca, pompy insulinowe lub glukometry. Mogą komunikować się z innymi urządzeniami (takimi jak smartfony) lub dostawcami usług opieki zdrowotnej, aby udostępniać podstawowe parametry życiowe lub ostrzegać o sytuacjach awaryjnych. Podsłuchiwanie sieci może pomóc zapewnić niezawodność i bezpieczeństwo tych urządzeń, a także zidentyfikować wszelkie potencjalne luki w zabezpieczeniach lub zagrożenia. Pojazdy autonomiczne: Pojazdy autonomiczne to urządzenia IoT,

które mogą samodzielnie się poruszać bez ingerencji człowieka, wykorzystując czujniki, kamery i GPS do nawigacji po otoczeniu. Mogą komunikować się z innymi pojazdami lub infrastrukturą w celu wymiany informacji lub koordynowania działań. Podsłuchiwanie sieci może pomóc w ocenie wydajności i bezpieczeństwa tych pojazdów, a także w wykrywaniu wszelkich złośliwych ataków lub zakłóceń.

To tylko kilka przykładów urządzeń IoT lub scenariuszy, w których sniffing sieciowy może być pomocny lub pouczający. Istnieje wiele innych zastosowań i przypadków użycia analizy sieci w domenie IoT.

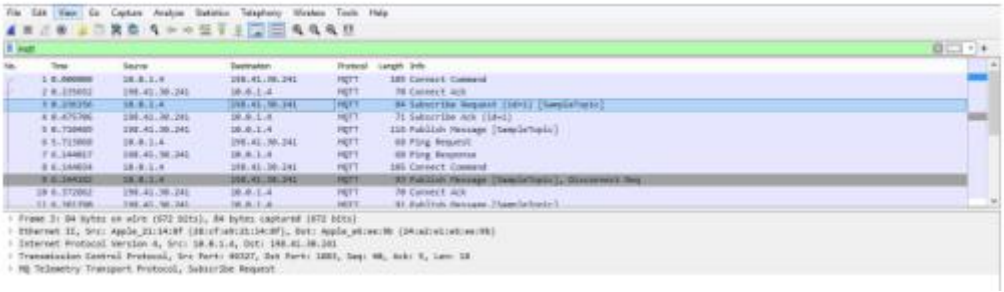
Podsłuchiwanie ruchu urządzeń IoT

Podsłuchiwanie ruchu sieciowego z urządzeń IoT za pomocą Wiresharka jest możliwe i może dostarczyć cennych informacji na temat protokołów komunikacyjnych oraz danych wymienianych między urządzeniami a ich serwerami. Poniżej przedstawiono kroki, jak podsłuchiwać ruch urządzeń IoT za pomocą Wiresharka:

1. Skonfiguruj środowisko sieciowe: Upewnij się, że komputer z uruchomionym Wiresharkiem jest podłączony do tej samej sieci, co urządzenia IoT, które chcesz monitorować. Może to być lokalna sieć Wi-Fi lub sieć LAN.

2. Rozpocznij przechwytywanie pakietów: Po wybraniu odpowiedniego interfejsu sieciowego kliknij przycisk „Start" w Wireshark, aby rozpocząć przechwytywanie pakietów. Domyślnie Wireshark przechwytuje cały ruch sieciowy na wybranym interfejsie.

3. Filtrowanie pakietów: Ponieważ urządzenia IoT mogą generować duży wolumen ruchu sieciowego, warto zastosować filtry w Wireshark, aby skupić się na konkretnych urządzeniach lub protokołach, którymi jesteś zainteresowany. Możesz użyć filtrów wyświetlania, takich jak adresy IP lub określone protokoły, takie jak MQTT lub CoAP, aby zawęzić zakres przechwyconych pakietów, jak pokazano na rysunku 2:



4. Analiza przechwyconych pakietów: Po przechwyceniu pożądanych pakietów można je przeanalizować za pomocą różnych funkcji Wiresharka. Można przeglądać szczegóły pakietów, wyświetlać informacje specyficzne dla protokołu, wyodrębniać ładunki danych, a nawet śledzić strumienie TCP, aby uzyskać pełniejsze zrozumienie komunikacji.

5. Interpretacja wyników: Analiza przechwyconych pakietów może dostarczyć informacji na temat wzorców komunikacji, formatów danych i aspektów bezpieczeństwa urządzeń IoT. Można wyszukiwać wzorce, anomalie lub potencjalne luki w zabezpieczeniach w ruchu, aby lepiej zrozumieć działanie urządzeń.

Analiza ruchu urządzeń IoT

Wireshark pomaga nam przechwytywać i analizować pakiety danych wysyłane i odbierane przez urządzenia IoT w sieci. Jednym z powszechnych sposobów wymiany danych między urządzeniami IoT jest użycie protokołu o nazwie Message Queue Telemetry Transport (MQTT), który jest lekkim i wydajnym protokołem działającym na bazie protokołu transportowego TCP i wykorzystuje model komunikacji typu publikuj-subskrybuj. W tym modelu urządzenia IoT mogą albo publikować dane w temacie, który jest etykietą identyfikującą typ danych, albo subskrybować temat, co oznacza, że chcą otrzymywać dane z tego tematu. Na przykład czujnik temperatury może publikować dane w temacie o

nazwie temp, a inteligentny termostat może subskrybować ten temat, aby odpowiednio dostosować system ogrzewania lub chłodzenia. Aby koordynować komunikację między wydawcami a subskrybentami, MQTT wykorzystuje centralny komponent zwany brokerem MQTT, który działa jako hub odbierający wszystkie opublikowane wiadomości i dystrybuujący je do zainteresowanych subskrybentów. Broker MQTT zarządza również połączeniami i subskrypcjami urządzeń IoT oraz zapewnia niezawodne dostarczanie wiadomości. Urządzenia IoT mogą implementować MQTT na dwa sposoby: MQTT Direct i MQTT przez Websockety. MQTT Direct to najprostszy sposób, w którym urządzenia łączą się bezpośrednio z brokerem MQTT za pomocą gniazd TCP. MQTT przez Websockety to kolejna metoda, w której urządzenia łączą się z brokerem MQTT za pomocą Websocketów, protokołu umożliwiającego dwukierunkową komunikację przez HTTP. Ta metoda może być bezpieczniejsza, ponieważ może używać certyfikatów do uwierzytelniania połączenia, a także bardziej kompatybilna z niektórymi sieciami korporacyjnymi, które mają ścisłe zapory sieciowe blokujące inne protokoły. W tym eksperymencie skupimy się na wykorzystaniu MQTT Direct do analizy ruchu urządzeń IoT za pomocą Wiresharka.

MQTT Direct

W MQTT Direct istnieje broker MQTT, który nasłuchuje na porcie 1883. Subskrybentami w tej sieci są wszystkie podłączone do niego urządzenia IoT, a także serwery, które mogą nasłuchiwać wiadomości w celu rejestrowania lub raportowania. Gdy urządzenie chce zasubskrybować brokera, podaje swój identyfikator klienta i określa temat, którego chce nasłuchiwać. Opcjonalnie urządzenie może również uwierzytelnić się za pomocą nazwy użytkownika i hasła. Podobnie, wydawca łączy się z brokerem za pomocą swojego identyfikatora klienta i określa temat, w którym chce opublikować wiadomość. Temat ten można traktować jako kanał, który pomaga uporządkować wiadomości wymieniane w sieci.

Zrozumienie komunikacji MQTT

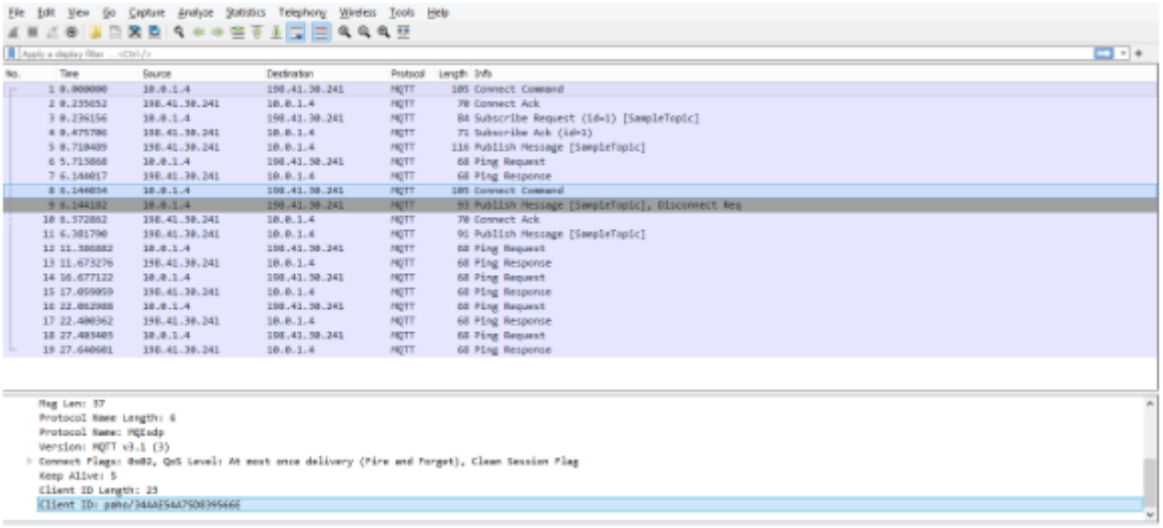
MQTT Direct to metoda wykorzystania protokołu MQTT, w której klienci MQTT komunikują się bezpośrednio z brokerem MQTT za pomocą gniazd TCP na porcie 1883. Klientami MQTT są dowolne urządzenia IoT lub serwery, które chcą udostępniać sobie nawzajem dane lub wiadomości. Broker MQTT jest centralnym komponentem, który zarządza komunikacją między klientami i zapewnia dostarczanie wiadomości. Aby skorzystać z MQTT Direct, klienci muszą wykonać kilka kroków: Najpierw muszą wysłać polecenie połączenia (connect) do brokera, które zawiera ich identyfikator klienta oraz, opcjonalnie, nazwę użytkownika i hasło do uwierzytelnienia. Identyfikator klienta to unikalny identyfikator, który odróżnia każdego klienta od innych. Broker odpowie komunikatem „connack", aby potwierdzić połączenie.

Po drugie, muszą wysłać do brokera „żądanie subskrypcji" (subscribe request), w którym podają tematy, które chcą subskrybować, oraz poziom jakości usług (QoS) pożądany dla każdego tematu. Temat to etykieta identyfikująca typ danych lub wiadomości, a poziom QoS decyduje, ile razy i w jakiej kolejności wiadomości są dostarczane. Broker odpowie komunikatem „subback", aby wyrazić zgodę na subskrypcję.

Po trzecie, mogą wysyłać lub odbierać komunikaty „publish" do lub od brokera, który zawiera dane lub ładunek wiadomości oraz temat, do którego należy. Broker wysyła opublikowane wiadomości do wszystkich klientów subskrybujących dany temat, zgodnie z ich poziomem QoS. Broker może również wysyłać komunikaty „puback", „pubrec", „pubrel" lub „pubcomp", aby potwierdzić lub poprosić o retransmisję komunikatów publish, w zależności od poziomu QoS. Aby pokazać, jak działa MQTT Direct, przyjrzyjmy się przykładowi podgrzewacza IoT, który komunikuje się z serwerem swojego producenta za pomocą Wiresharka. To narzędzie przechwytuje i analizuje ruch sieciowy.

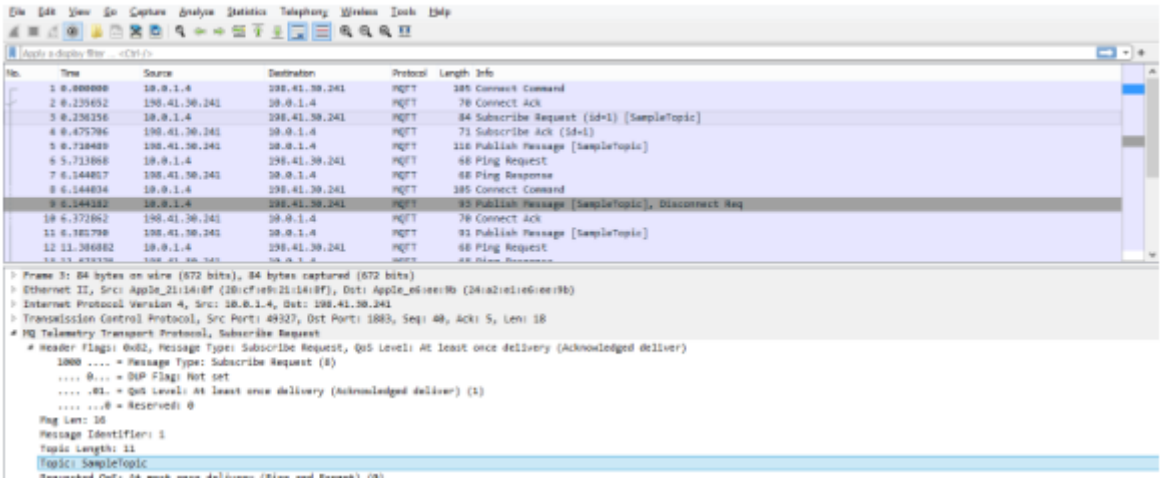
Polecenie Connect

Pierwszym pakietem w Wireshark jest polecenie „connect” wysyłane przez grzejnik do brokera. Widzimy, że ma on identyfikator klienta paho/34AAE54A75D839566E, co oznacza, że korzysta z biblioteki o nazwie Paho do komunikacji MQTT, jak widać na rysunku 3:



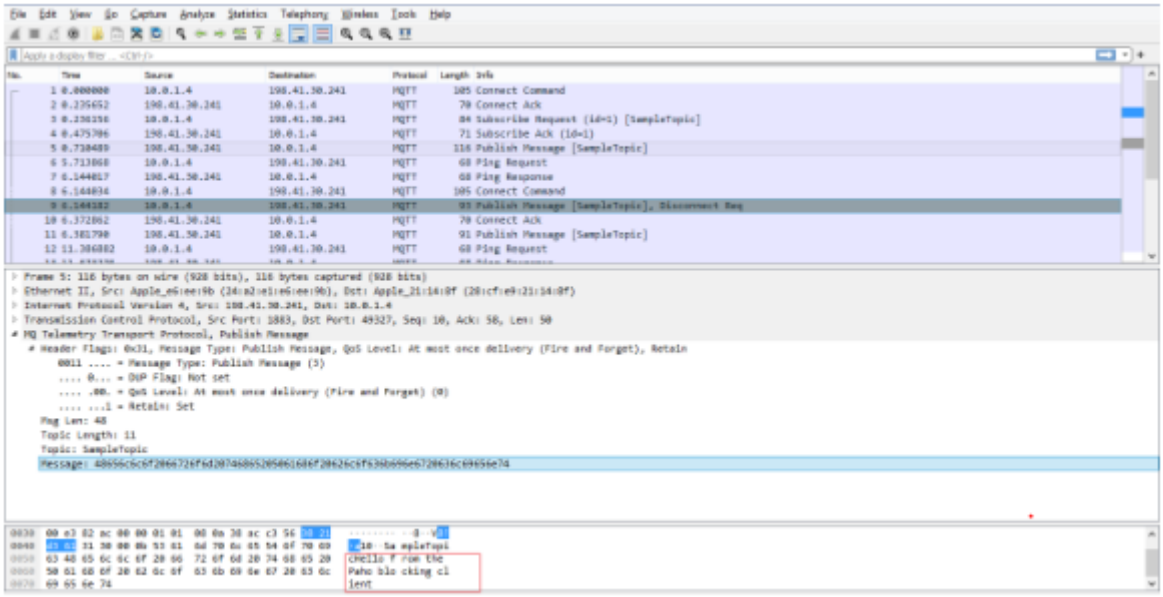
Żądanie subskrypcji

Kolejny pakiet, który widzimy, to żądanie subskrypcji wysłane przez podgrzewacz do brokera. Widzimy, że chce on zasubskrybować temat o nazwie „SampleTopic” z poziomem QoS równym 0, jak pokazano na rysunku .4. Oznacza to, że chce tylko jednokrotnego dostarczenia każdej wiadomości bez potwierdzenia od brokera.



Publikuj wiadomość

Ostatnim pakietem, który widzimy, jest wiadomość publikująca wysłana przez brokera do podgrzewacza. Widzimy, że zawiera ona temat Sampletopic i treść „Hello from the Paho blocking client”, jak widać na rysunku 5, co oznacza, że jest to wiadomość od innego klienta korzystającego z Paho, który również subskrybuje ten temat.



Ten przykład pokazuje, jak nagrzewnica łączy się z serwerem producenta, subskrybuje temat w celu pobierania poleceń i danych oraz odbiera wiadomość od innego klienta za pomocą protokołu MQTT Direct. Pomaga nam to zrozumieć, jak urządzenia IoT wykorzystują protokół cMQTT do efektywnej i niezawodnej komunikacji.

Wnioski

W tym rozdziale poznaliśmy koncepcję i funkcje urządzeń IoT oraz ich protokołów komunikacyjnych. Poznaliśmy również kilka przypadków użycia sniffingu sieciowego urządzeń IoT w różnych domenach i scenariuszach. Ponadto dowiedzieliśmy się, jak używać programu Wireshark do przechwytywania i analizowania ruchu urządzeń IoT. Skupiliśmy się na jednym z popularnych protokołów komunikacyjnych wykorzystywanych przez urządzenia IoT: MQTT Direct. Dowiedzieliśmy się również, jak używać programu Wireshark do interpretowania i wizualizacji danych o ruchu urządzeń IoT. W kolejnym rozdziale skupimy się na tym, jak używać programu Wireshark do wykrywania ataków sieciowych. Przedstawimy kilka typowych rodzajów ataków sieciowych i pokażemy, jak używać programu Wireshark do ich identyfikacji i obsługi. Pod koniec następnego rozdziału będziesz w stanie używać Wiresharka do monitorowania ruchu sieciowego i wykrywania wszelkich podejrzanych lub złośliwych zachowań

Pytania

1. Co oznacza skrót IoT?

a) Internet rzeczy

b) Internet technologii

c) Internet transakcji

d) Internet telekomunikacji

2. Jakie są główne komponenty ekosystemu IoT?

a) Urządzenia, czujniki, siłowniki, kontrolery i interfejsy

b) Urządzenia, serwery, bazy danych, narzędzia analityczne i pulpity nawigacyjne

c) Urządzenia, protokoły, standardy, frameworki i polityki

d) Urządzenia, bramy, sieci, platformy, aplikacje i użytkownicy

3. Czym jest architektura IoT?

a) Graficzna reprezentacja przedstawiająca fizyczny układ i połączenia komponentów IoT

b) Logiczny projekt definiujący przepływ danych i przetwarzanie komponentów IoT

c) Model warstwowy opisujący funkcje i interakcje komponentów IoT

d) Struktura hierarchiczna, która organizuje komponenty IoT

w grupy i podgrupy

4. Jak działa IoT? a) Poprzez szyfrowanie, kompresję, przechowywanie, pobieranie i usuwanie danych z urządzeń IoT

b) Poprzez gromadzenie, przesyłanie, przetwarzanie, analizowanie i przetwarzanie danych z urządzeń IoT

c) Poprzez generowanie, nadawanie, odbieranie, filtrowanie i wyświetlanie danych z urządzeń IoT

d) Poprzez walidację, weryfikację, uwierzytelnianie, autoryzację i audyt danych z urządzeń IoT

5. Jakie są korzyści płynące z IoT?

a) Wydajność, wygoda, innowacyjność i tworzenie wartości

b) Bezpieczeństwo, prywatność, niezawodność i skalowalność

c) Różnorodność, inkluzywność, dostępność i przystępność cenowa

d) Jakość, ilość, różnorodność i dostępność

6. Jakie są przykłady zastosowań sniffingu sieciowego urządzeń IoT? a) Inteligentne domy, inteligentne miasta, opieka zdrowotna, rolnictwo, przemysł i transport

b) Gry, rozrywka, edukacja, media społecznościowe, e-commerce i bankowość

c) Pogoda, klimat, środowisko, energia, zarządzanie klęskami żywiołowymi i reagowanie kryzysowe

d) Wszystkie powyższe

7. Czym jest sniffing sieciowy?

a) Metoda monitorowania i kontrolowania ruchu sieciowego i przepustowości wykorzystywanej przez urządzenia w sieci.

b) Proces skanowania i wykrywania luk w zabezpieczeniach sieci i zagrożeń stwarzanych przez urządzenia w sieci.

c) Narzędzie do konfigurowania i zarządzania ustawieniami sieciowymi oraz preferencjami stosowanymi do urządzeń w sieci.

d) Technika przechwytywania i analizowania pakietów danych wysyłanych i odbieranych przez urządzenia w sieci.

8. Czym jest Wireshark?

a) Narzędzie do symulacji sieci, które może tworzyć i testować różne scenariusze ruchu sieciowego.

b) Narzędzie do wizualizacji sieci, które może generować i wyświetlać wykresy i diagramy ruchu sieciowego.

c) Narzędzie do analizy sieci, które może przechwytywać i wyświetlać pakiety danych ruchu sieciowego.

d) Narzędzie do optymalizacji sieci, które może poprawić i zwiększyć wydajność oraz jakość ruchu sieciowego.

9. Czym jest MQTT Direct?

a) Sposób wykorzystania protokołu MQTT, w którym urządzenia IoT łączą się bezpośrednio z brokerem MQTT za pomocą gniazd TCP na porcie 1883.

b) Sposób wykorzystania protokołu MQTT, w którym urządzenia IoT łączą się z brokerem MQTT za pomocą gniazd WebSocket na porcie 80 lub 443.

c) Sposób wykorzystania protokołu MQTT, w którym urządzenia IoT łączą się ze sobą bez użycia brokera MQTT na żadnym porcie.

d) Sposób wykorzystania protokołu MQTT, w którym urządzenia IoT łączą się z usługą w chmurze, która działa jako broker MQTT na dowolnym porcie.

10. Na czym polega model komunikacji typu publikuj-subskrybuj w MQTT?

a) Model, w którym urządzenia IoT mogą żądać danych z tematu lub odpowiadać tematowi, przesyłając mu dane.

b) Model, w którym urządzenia IoT mogą publikować dane w temacie lub subskrybować temat, aby odbierać z niego dane.

c) Model, w którym urządzenia IoT mogą wysyłać dane do tematu lub odbierać dane z tematu w kolejności sekwencyjnej.

d) Model, w którym urządzenia IoT mogą transmitować dane do tematu lub nasłuchiwać danych z tematu.

Odpowiedzi

1. a

2. d

3. c

4. b

5. a

6. d

7. d

8. c

9. a

10. b