Sławomir Sowa, Michał Durski
Intelligia sp. z o.o.

Cyberbezpieczeństwo w automatyce obiektowej

Wdobie tak intensywnego rozwoju technologii i cyberprzestrzeni zapewne każdy z nas dostrzega liczne zalety, jakie ten proces niesie ze sobą. Innowacyjne urządzenia pozwalają na monitorowanie czynności naszych organizmów, inteligentne samochody zyskują coraz większą autonomię, a systemy automatyki w naszych domach umożliwiają kontrolę i sterowanie instalacjami w budynku za pomocą jednego kliknięcia w aplikacji mobilnej.

Powinniśmy jednak pamiętać o niebezpieczeństwach związanych z tak postępującą cyfryzacją naszego życia, a co za tym idzie - również danych personalnych i prywatności.

Raport „The Future Smart Home: 500 Smart Objects Will Enable New Business Opportunities“, przeprowadzony przez firmę Gartner wykazał, że do 2022 r. w typowym domu będzie znajdowało się nawet 500 inteligentnych urządzeń.


Fot. freeimages.com

Każde urządzenie łączące się z siecią internetową pozostawia ślad cyfrowy. Tym samym, może stać się celem cyberataku.

Może być to smart TV, inteligentna lodówka, ekspres do kawy, czy budzik, ale także system grzewczy, oświetleniowy, alarmowy, czy przeciwpożarowy.

Cyberprzestępcy są w stanie wykorzystać nawet niepozorny budzik, łączący się z naszym smartphone jako podsłuch. Inteligentny telewizor może stać się narzędziem do podglądania domowników, celem chociażby przeprowadzenia kradzieży w ich domu.

Warto więc być świadomym nowych zagrożeń i dokonywać wyboru systemów i urządzeń posiadających możliwie najlepsze zabezpieczenia sieciowe.

Przyjrzyjmy się najważniejszym z nich w kontekście inteligentnego domu.

Jeszcze nie tak dawno korzystaliśmy z internetu bez protokołu **SSL (protokół szyfrowania danych między klientem, a serwerem)**. Obecnie stosowane są bardziej zaawansowane rozwiązania szyfrujące, jakie chociażby możemy spotkać w **Web3.**

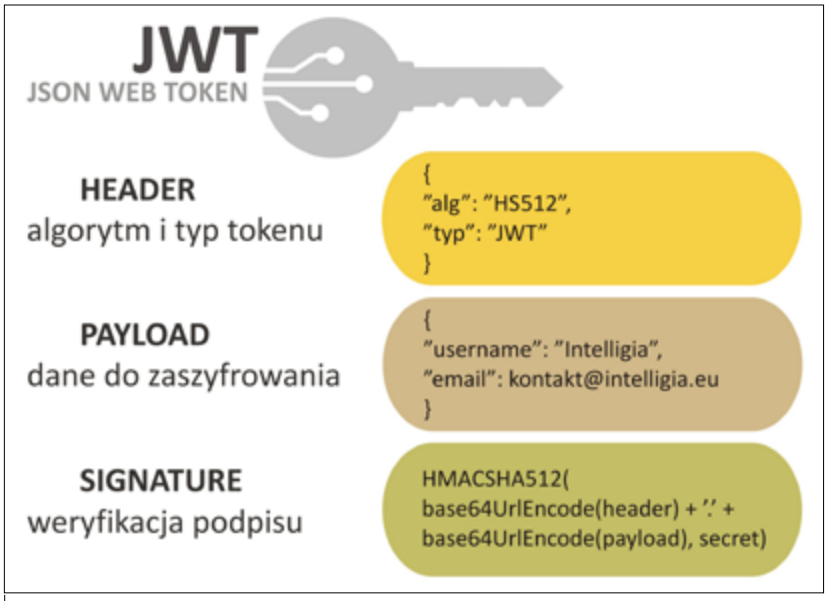
Internet wersji trzeciej, w najprostszym ujęciu, jest to zdecentralizowany system przechowywania danych. W tej wersji dane te są własnością użytkownika. Obecnie dane te są własnością właściciela serwera, przez co istnieje możliwość wycieku danych do sieci w momencie ewentualnej awarii, bądź niepowołanej autoryzacji. W konsekwencji obecnie proponowane, jak i wdrażane rozwiązania zapewniają niską awaryjność systemu i wysoki poziom bezpieczeństwa danych dla użytkowników „rozwiązań inteligentnych" - ale i nie tylko. Jest to bardzo istotne z punktu widzenia systemów automatyki budynkowej, które coraz częściej posiadają pełną możliwość kontroli, sterowania poprzez aplikacje internetowe, bądź aplikacje natywne. Dostęp do kontroli i sterowania zdalnego budynku, to nie tylko wygoda i komfort dla użytkownika. To również niebezpieczeństwo przejęcia kontroli nad systemem sterowania przez osoby nieuprawnione. Aktualnie systemy automatyki obiektowej związane z IoT (**Internet rzeczy**) są uruchomione najczęściej na serwerze umiejscowionym na hali (w przypadku firm), bądź w pomieszczeniach budynku, domu klienta.

Dane znajdujące się na dyskach mogą zawierać informacje odnoszące się do kluczy dostępowych, danych identyfikacyjnych, bądź innych wrażliwych informacji. Dzięki zastosowaniu najnowszych technologii jesteśmy w stanie zminimalizować pewnego rodzaju ryzyko autoryzacji osób niepowołanych.

Jednym z możliwych do zastosowania systemów jest **blockchain**.

Jest to rozproszony system, który umożliwia rozłożenie różnych danych w wielu miejscach. Dostęp do jednego z tych miejsc nie umożliwia nam odczytania zawartości danych bez mechanizmu konsensu, który składa wszystkie informacje w całość oraz bez dostępu wszystkich wymaganych informacji.

W ten sposób możemy zabezpieczyć dane ustawień systemowych i użytkowników, przechowywane w urządzeniach wykonawczych systemu automatyki budynkowej. Pozostaje jeszcze kwestia bezpieczeństwa przesyłu danych pomiędzy różnymi urządzeniami w danym systemie sterowania.



Rys. 1. Budowa tokenu autoryzacyjnego JWT

Problem ten można rozwiązać na wiele sposobów. Specjaliści od projektowania zabezpieczeń w przesyłaniu danych, wprowadzają szereg nowych rozwiązań, posiadających coraz wyższe współczynniki zabezpieczenia dostępu z zewnątrz do naszego systemu.

Obecnie dane przesyłamy między serwerem automatyki, a klientem na podstawie protokołu **HTTP**, bądź **WebSocket**, Dzieje się tak w przypadku wymiany informacji na żywo. Protokół HTTP możemy zabezpieczyć chociażby za pomocą protokołu sieciowego **SSL**.

Token autoryzacyjny JWT

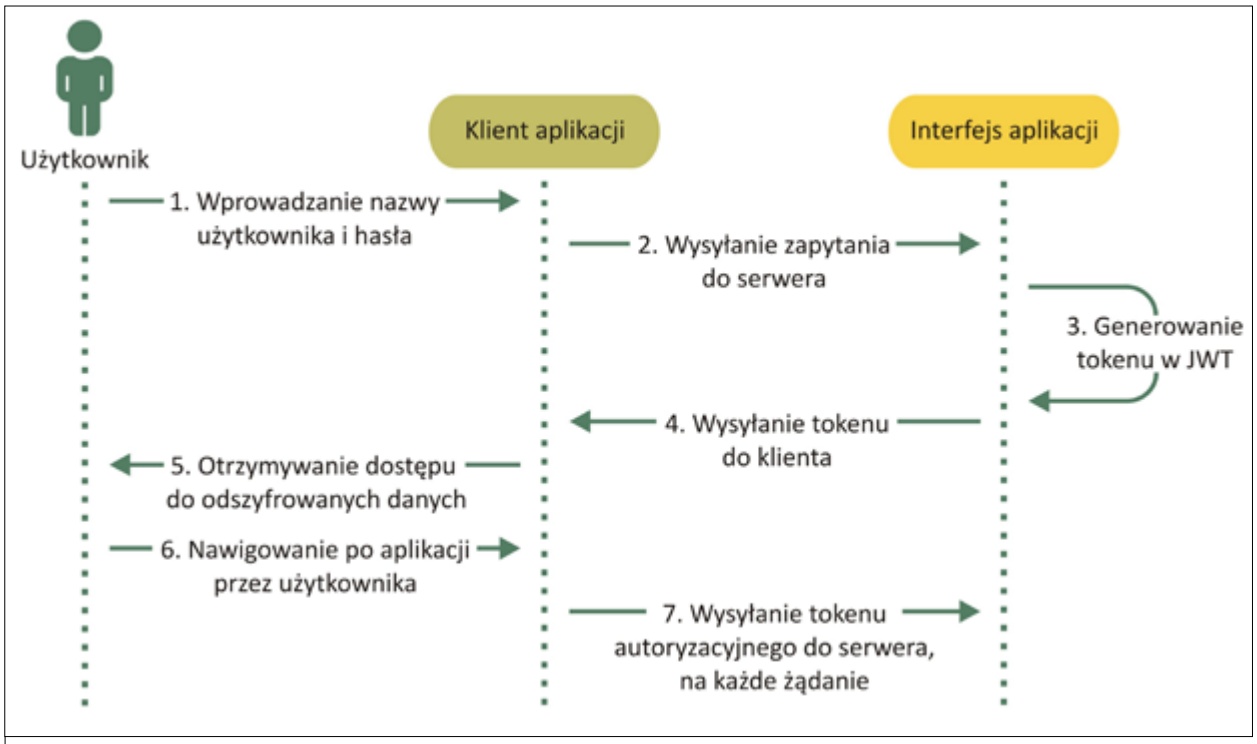
WebSocket zabezpieczamy za pomocą mechanizmu sesji, bądź tokenizacji jakim jest np. token posiadacza [**JWT - (Json Web Token)**]. Token ten jest powszechnie używany do uwierzytelniania zaszyfrowanych danych. Na rysunku 1 przedstawiono budowę tokenu autoryzacji JWT, w którego skład wchodzą trzy bloki:

- Header, czyli nagłówek, który zawiera określenia dla tokenu oraz algorytmu szyfrującego,
- Payload, który jest informacją do zaszyfrowania danych dotyczących użytkownika/ domownika korzystającego z systemu automatyki obiektowej,
- Signature, w którym mieści się podpis tokenu.

Odrębnym również popularnym rozwiązaniem jest **OAuth**, którego wykorzystuje jeden z czołowych portali społecznościowych. Do tego możemy dodać mechanizmy podpisu z blockchain-u w celu uwierzytelnienia, że „my to my" dla serwera i voilà. Jest to jeden z przykładów dobrego zabezpieczenia transmisji danych dla automatyki.

Mechanizmy uwierzytelniania w aplikacji

Do uwierzytelniania aplikacji wykorzystuje się różne sposoby szyfrowania danych w celu ich ochrony. W systemach automatyki budynkowej wykorzystujemy mechanizmy uwierzytelniania danych. Zabezpiecza to inteligentna instalacja budynkowa przed dostępem



Rys. 2. Schemat wykorzystania mechanizmu tokenizacji w aplikacji

osób niepowołanych do konfiguracji, ustawień systemów automatyki obiektowej. Na rysunku 2 znajduje się poglądowy schemat funkcjonowania mechanizmów uwierzytelniania użytkownika. Opiera się on na algorytmie szyfrowania danych, które wykorzystywane są na całym świecie. Możemy wyróżnić dwa podstawowe mechanizmy szyfrowania AES (Advanced Encryption Standard, który w oryginalnej nazwie brzmi Rijndael) oraz SHA-256 (Secure Hash Algorithm). Mimo, że mechanizm powstał na przełomie ubiegłego wieku, powszechność jego używania jest postrzegana jako najwyższy standard bezpieczeństwa w obecnych czasach. Niezależnie od tego prowadzone są czynności zmierzające do jeszcze wydajniejszej i bezpieczniejszej pracy tych systemów szyfrujących. Zabezpieczenie naszych danych sterujących automatyką budynkową staje się bardzo ważne, gdy chcemy - jako użytkownicy - mieć dostęp do monitorowania stanu pracy oraz sterowania systemu automatyki obiektowej z zewnątrz. Wykorzystywane są do tego celu komputery, tablety, smartfony, a medium pośredniczącym jest sieć internetowa. W celu osiągnięcia jak najwyższego poziomu bezpieczeństwa danych można wykorzystać rozwiązania chmurowe, które ułatwią nam sprawę z konfiguracją, jak i utrzymaniem spójnej infrastruktury.

Istnieje także możliwość wykonania własnej implementacji kontroli lokalnego serwera w sieci zewnętrznej. Wówczas konieczny jest kontakt z naszym dostawcą internetu w celu zapewnienia statycznego adresu IP. Można także posłużyć się innymi rozwiązaniami związanym z rozproszonym systemem nazw sieciowych **DNS**. Dodatkowo dochodzi jeszcze kwestia zabezpieczenia portów, bądź implementacja systemów anty **DDoS**.

Podsumowanie

Zwiększająca się popularność i dynamiczny rozwój różnego rodzaju systemów inteligentnej automatyki obiektowej, wymusza opracowywanie coraz lepszych metod zabezpieczania danych kontrolujących i sterujących inteligentnym budynkiem. Kwestia zabezpieczania dostępu do systemu sterowania, wydaje się być kluczowa i zapewne będzie poddawana licznym usprawnieniom.

W zagadnieniach związanych z bezpieczeństwem systemów inteligentnego sterowania budynkami, najbardziej stabilne jest bezpieczeństwo techniczne, Jest tak ze względu na to, że jest ono probabilistycznie przewidywalne. Można w miarę dokładnie określić jakie urządzenia i kiedy mogą ulec uszkodzeniu.

Z drugiej strony, największym problemem jest człowiek, a konkretnie jego zamierzone, destrukcyjne działanie, zmierzające do przejęcia kontroli nad zaawansowanymi systemami sterowania budynków. Często, dla zwiększenia skuteczności działania, użytkownicy tych systemów nie mają świadomości o stopniu zaawanasowana użytych technologii służących do ochrony systemu, które zostały zaimplementowane przez instalatorów. □