Ireneusz Maj

Internet : rzeczy i zagrożenia z nimi związane

Bezpieczeństwo : teoria i praktyka : czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 9/3, 51-57

2015

BEZPIECZEŃSTWO • 2015 nr 3 TEORIA I PRAKTYKA

Ireneusz Maj*

Internet rzeczy i zagrożenia z nim związane

Wprowadzenie

Zjawiskiem, które określa Internet rzeczy (ang. *Internet of Things*) jest przekaz danych informacji między przedmiotami i ludźmi lub tylko między przedmiotami. Internet, jest medium komunikacyjnym, platformą wymiany danych i informacji. Internet rzeczy[1] jest koncepcją, w której przedmioty mogą za pośrednictwem sieci komputerowej gromadzić, przetwarzać i wymieniać dane. Internet rzeczy umożliwia komunikację nie tylko między przedmiotami, urządzeniami i ludźmi, ale także między samymi przedmiotami i urządzeniami. Gromadzenie, przetwarzanie i wymiana ograniczone tylko do obszaru urządzeń określamy węższym pojęciem M2M[2]. Należy zwrócić uwagę, że wcześniej, gdy mówiono o zdalnym odczycie danych licznika elektrycznego, przyjmowaliśmy stan, w którym raz w miesiącu lub rzadziej nastąpi odczytanie stanu zużycia energii. W środowisku Internetu rzeczy mamy sytuację, kiedy online w czasie rzeczywistym, nie tylko odczytujemy zużycie, ale możemy – przez sformułowanie określonych algorytmów − oczekiwać danych o minimalnych i maksymalnych zużycia w określonych okresach, o obecności w domu mieszkańców, o porach największego zużycia energii, przeliczonych kosztach zużycia, a nawet – w myśl zadanej procedury – np. brak płatności za rachunki, dokonać zdalnego wyłączenia.

* Doktor filozofii, Mehle Polska.

1 Przyjmuje się, że z Internetem rzeczy mamy do czynienia od momentu, gdy liczba urządzeń podłączonych do sieci przekroczyła liczbę ludności na Ziemi. Termin „Internet rzeczy, czy Internet przedmiotów" (Internet of Thincs – IoT) został po raz pierwszy użyty przez Kevina Ashtona w tytule prezentacji, jaką zrobił w Procter & Gamble (P&G) w 1999 roku. Prezentacja dotyczyła nowego pomysłu łączącego RFID z łańcuchem łańcucha dostaw. http://www.rfidjournal.com/articles/view?4986.

2 M2M – skrót od słów w języku angielskim Machine to Machine.

Ważną cechą przedmiotów w Internecie rzeczy, którą w literaturze – głównie technicznej – przyjmuje się jako naturalną, jest jednoznaczna identyfikowalność przedmiotu. Przedmiot musi posiadać swój adres IP![3]

Przejście od tradycyjnego produktu np. telewizora, sprzętu AGD, do produktów inteligentnych, które w Internecie rzeczy, przez sieć, będą generować nowe usługi, spowodowało i powoduje zmianę modelu prowadzenia biznesu. Zmienia się model komunikacji z klientem. Urządzenia poprzez Internet rzeczy będą dla klientów dedykować nowe usługi. Według różnych źródeł, rynek Internetu przedmiotów stanie się największym rynkiem urządzeń na świecie. Samsung zapowiedział, że do 2017 roku wszystkie jego telewizory będą urządzeniami IoT[4]. Podobnie LG w obszarze inteligentnych domów produkuje telewizory i sprzęt AGD mogące łączyć się z Internetem. Obszarem Internetu rzeczy[5], który rozwija się bardzo dynamicznie, jest M2M. W rozwoju gospodarki M2M staje się kluczową technologią i głównym obszarem rozwoju usług internetowych związanych z tą technologią. M2M odnosi się do technologii komunikowania przewodowo i bezprzewodowo miedzy urządzeniami stanowi integralna część Internetu. Zakres zastosowań technologii M2M obejmuje automatykę przemysłową, logistykę (telematykę), inteligentne sieci, miasta, służbę zdrowia, energetykę, monitoring, obszar związany z obronnością oraz całą sferę kontroli[6]. Wcześniej komunikacja odbywała się między konkretnymi, najczęściej dwoma, urządzeniami (odczyt temperatury, stan paliwa, ciśnienie, szybkość przepływu czynnika płynnego, stan zapasów).

Dzisiaj komunikacja taka ma charakter już sieci urządzeń z urządzeniem centralnym, w układzie rozproszonym lub układem urządzeń zarządzanym w chmurze[7]. Sieci bezprzewodowe, które wzajemnie się przenikają, uzupełniają pozwalają na komunikację w sferze produkcji, optymalizacji zapasów i automatycznego procesu ich uzupełniania, monitoringu urządzeń i konserwacji w tym aktualizacji oprogramowania.

---

[3] Zapotrzebowanie, w związku miedzy innymi na Internet rzeczy, na adresy IP protokołu w wersji czwartej IPv4, spowodowało praktyczne wyczerpanie tej wersji i z tego powodu powstała szósta wersja protokołu IPv6.

[4] IoT – Internet rzeczy.

[5] I. Maj, *E-gospodarka a Interent Rzeczy*, [w:] *E-gospodarka w Europie Środkowej i Wschodniej. Teraźniejszość i Perspektywy Rozwoju*, red. S. Partycki, Lublin 2015.

[6] Problem M2M i Internetu rzeczy jest rosnące nieliniowo zapotrzebowanie na przestrzeń adresową. Obecna podaż wskazuje, że w niedługim czasie należałoby wdrożyć protokół IPv6, który zapewni dynamiczny rozwój technologii Internetu rzeczy.

[7] Jednym z pierwszych przykładów wykorzystania M2M było odczytanie numeru telefonu osoby dzwoniącej. W technologii GSM (Simens) wykorzystanie protokołu IP do komunikacji miedzy urządzeniami (stacjami). Później przychodzi następny etap wykorzystania bram i routerów bezprzewodowych. Po roku 2006 następuję dynamiczny rozwój urządzeń, które przetwarzają dane w żądany format danych, poddają dane obróbce według zadanych inteligentnych algorytmów. Sieci tych urządzeń, które selektywnie, w zależności od wyniku przetworzenia danych, same dokonują, miedzy innymi, wyboru adresata (oznaczane często są dla odróżnienia M2Mi). Następnie przychodzi moment, kiedy elementy sieci w technologii M2M są zarządzane w czasie rzeczywistym w celu poprawy efektywności wykorzystania sieci i poprawy szybkości przepływu danych. Innym nowym wdrożeniem M2m jest łączność w sieciach komórkowych w chmurze. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, *Internet of Things (IoT): A vision, architectural elements, and future directions*, "Future Generation Computer Systems", September 2013, Vol. 29, s. 1645–1660.

Innym obszarem wykorzystania technologii M2M jest kontrola i monitoring liczników: liczników poboru energii elektrycznej, gazu, wody zimnej i ciepłej, poboru ciepła. Jeszcze innym interesującym zastosowaniem jest wymiana automatyczna treści zamieszczanej na komunikatorach, tak ze względu na czas emisji, jak i automatycznego wyboru grupy docelowej, do której wybrane treści komunikatów są adresowane[8].

Ilość aplikacji w obszarze M2M rośnie w postępie chyba geometrycznym od wąskich dedykowanych zastosowań, często bardzo wyrafinowanych zastosowań wojskowych, do nieprzeliczalnej ilości zastosowań ogólnych[9].

Przed Internetem rzeczy są i staną następujące problemy[10]:

- Wielość danych dla użytkownika może stanowić problem z ich absorbowaniem, problem z ich interpretacją. Właściwym kierunkiem będzie podawanie informacji już przetworzonej automatycznie przez przedmiot w prostej, zrozumiałej formie. Odrębnym problemem jest dostosowanie szybkości przetwarzania informacji w odpowiednią formę komunikatu i przekazaniu go w odpowiednim czasie dla odbiorcy[11].
- Obecnie telewizory połączone z Internetem przekazują wiele dodatkowych informacji i komunikatów. W nieodległym czasie Internet rzeczy, po analizie preferencji, wskaże nam właściwy program, odpowiadający określonej porze dnia itd.
- Przed producentami tworzy się – poprzez Internet rzeczy – potencjalny, nowy nieograniczony obszar usług i użyteczności dla klienta.
- Tak po stronie producentów, jak i klientów stoi poważne wyzwanie badania i rozstrzygnięcia, które z nowych użyteczności wniosą coś istotnego w nasze codzienne życie, a które staną się zbędnym gadżetem. Już dzisiaj nawigacja po wielu urządzeniach wymaga wielu godzin nauki i ogromnej cierpliwości. Nadmiarowość funkcji, aplikacji stanowi istotne wyzwanie dla użytkownika. Sfera ergonomii urządzenia zostaje na dalszym planie. Stąd w obszarze Internetu rzeczy nawigacja po mapie możliwości, setek możliwych do wykorzystania aplikacji, przystępnej informacji o korzyściach, jakie wynikają z zastosowania konkretnej aplikacji, staje się warunkiem *sine qua non* zadowolenia klienta.
- Ważnym wyzwaniem dla Internetu rzeczy jest, aby konkretne technologie rozwiązywały autentyczne problemy. Aby oferowana technologia nie była iluzją wyimaginowanych potencjalnych potrzeb.
- Niezwykłe istotne jest, aby w Internecie rzeczy producenci wybierali problemy do rozwiązania, które mają statystycznie szczególny wymiar zastosowania. Są uzasadnione obawy, że Internet rzeczy będzie generował podobne problemy z użytecznością, jak rynek urządzeń ubieralnych[12].

---

[8] Zdarzeniami z obszaru M2M w telefonii komórkowej są przykładowo wszelkie automatyczne powiadomienia operatora i innych usługodawców, którym udostępniliśmy tą formę komunikacji, ankiety sprawdzające elementy satysfakcji klienta, oferty itp.

[9] Osobnym problemem, w obszarze zastosowań Internetu rzeczy, jest RFID. RFID – Radio-frequency identification – jest techniką wykorzystującą fale radiowe do przesyłania danych, czy identyfikacji przedmiotu, obiektu.

[10] I. Maj, *op. cit.*

[11] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, *op. cit.*

[12] Urządzenia ubieralne (*wearable devices*), to miedzy innymi inteligentne bransoletki, opaski, pierścionki, zegarki, okulary, opaski, ubrania. Przykładowo biżuteria bezpieczeństwa Cuff, bransoletki

- Potencjalnym problemem Internetu rzeczy może być kwestia własności urządzenia. Po zakupie fizycznie jesteśmy jego posiadaczem, ale nie jest on w pełni naszą własnością. Pozostają do rozstrzygnięcia problemy: kto jest właścicielem zbieranych danych, czy są ograniczenia w przekazywaniu danych osobom i podmiotom trzecim, do jakiego momentu aktualizacje oprogramowania są bezpłatne – opłacone przy zakupie urządzenia, w jakim zakresie mamy dostęp do gromadzonych danych, czy zbierane dane stanowią dla nas zagrożenie, np. czy poprzez wydawanie poleceń głosowych możemy być pewni, że dane urządzenie nie przekazuje dalej wszystkich, bądź wybranych rozmów z pomieszczenia, w którym się znajduje. Wadą tego typu ekosystemów może być to, że to producent zdalnie będzie decydował o funkcjach udostępnianych przez urządzenie.
- W obszarze Internetu rzeczy nie mamy jeszcze wykształconych standardów, które zapewniłyby kompatybilność między urządzeniami różnych producentów. Brak standaryzacji i porozumienia między producentami powoduje, że przejście z urządzenia jednego producenta na urządzenie drugiego staje się poważnym wyzwaniem, nawet dla doświadczonego użytkownika.
- Nie nowym, ale ważnym problemem dla Internetu rzeczy jest interfejs. Nie ma określonego kierunku rozwoju metod komunikacji z urządzeniem. Można wyróżnić kilka trendów: sterowanie głosem, gestami, dotykiem, mimiką itp. Najbardziej intuicyjne wydaje się sterowanie głosem i gestami. Pozostaje do rozwiązania problem wielu urządzeń znajdujących się w jednym pomieszczeniu. Interesującym jest kierunek sterowania wszystkimi metodami równocześnie. Wspomaganie sterowania gestami, głosem i dotykiem.
- Zakładając, że większość rzeczy jest podłączona do sieci, stan ten ma wpływ na sposób tworzenia faktycznej wartości przedmiotu. W wielu przypadkach wartością już nie jest bezpośrednio sam przedmiot, ale raczej usługa wykonywana za pośrednictwem sieci, do której użytkownicy mają dostęp poprzez ten przedmiot.
- Niezawodność. Wraz ze stopniem skomplikowania urządzenia maleje jego niezawodność, rośnie koszt serwisu, a tym samym koszty użytkowania.

Internet rzeczy i zagrożenia z nim związane

Upowszechnienie rozwiązań Internetu rzeczy w niedalekiej przyszłości spowoduje istotne przemiany społeczne. Można założyć, że wzrośnie efektywność gospodarowania, zmaleją istotnie koszty produkcji, zmaleje zużycie energii, nastąpi optymalizacja w czasie rzeczywistym wykorzystania tak czasu, jak i zasobów. Jest raczej pewne, że systemy sztucznej inteligencji w technologii M2M, będą przejmować obszary podejmowania decyzji, dotąd zarezerwowane wyłącznie dla człowieka[13].

MEMI, koszulki OMsignal, bielizna Fundawear pierścionek Ringly. Ringly, to inteligentna ciekawa alternatywa dla kobiet wobec dostępnych na rynku zegarków, opasek i bransoletek dedykowanych, ze względu na swój design, mężczyznom. Ringly jest zsynchronizowany ze smartfonem i za pomocą wibracji informuje o przychodzących połączeniach.

[13] R.H. Weber, *Internet of Things – New security and privacy challenges*, „Computer Law & Security, Review", January 2010, Vol. 26, s. 23–30.

W tak objętościowo wielkim obszarze zjawisk, jakim jest Internet rzeczy, zagrożenia z nim związane nie poddają się prostej klasyfikacji. Bardzo obszerna literatura przedmiotu dotyczy obszaru problemów rozwiązań technicznych. Gdzieniegdzie wspomina się głównie o samym zjawisku, jak o potencjalnych produktach i usługach. Można wskazać na dwa naturalne obszary:

- zagrożenia o szeroko rozumianym charakterze społecznym;
- zagrożenia o charakterze technicznym (technologicznym).

Zagrożenia o charakterze społecznym związane z Internetem rzeczy, ze względu na fakt, że sam Internet stał się wszechobecnym medium komunikacyjnym, mają i będą mieć różnoraki charakter, podlegający ciągłym dynamicznym zmianom. Można wskazać na kilka takich zagrożeń będących zapowiedzią tego, co nas czeka:

- Bezrobocie. Tylko z racji odczytu liczników zużycia energii elektrycznej, gazu i prądu ubędzie kilkaset tysięcy miejsc pracy. W związku z zaawansowanymi technologicznie programami rozpoznawania mowy i semantycznym rozpoznawaniem stawianych pytań i budowania odpowiedzi nastąpi poważny spadek zatrudnienia w obszarach szeroko rozumianej informacji, w tym w firmach typu Call Center. Śledząc rozwój urządzeń ubieralnych mamy np. pełny odczyt online podstawowych parametrów pacjenta, jego lokalizację, z możliwością automatycznego podawania zaleceń, leków, w tym np. insuliny. Dalej: dzięki opasce mamy osobistego trenera i w tym dodatkowo pełny pomiar podstawowych parametrów podczas samodzielnego treningu, z automatycznym rozpoznaniem rodzaju wysiłku fizycznego: bieg, chód, spacer, z automatycznym wyliczeniem liczby spalonych kalorii, z możliwościami porównania z poprzednimi, analizą tych zapisów i możliwością automatycznego porównania z gronem znajomych swoich osiągnięć przez automatyczne udostępnienie np. przez portale społecznościowe[14]. Jeszcze innym obszarem eliminującym miejsca pracy jest zastępowanie konsultantów serwisowych oprogramowania użytkowego, portali użytkowych praktycznie wyłącznie obsługą programową np. Allegro. Podobnie będą generować bezrobocie wszelkiego typu usługi w rodzaju: monitoring, kontroling, automatyka, konserwacja oprogramowania, aktualizacja oprogramowania, logistyka, w tym telematyka.
- Zagrożenie bezpieczeństwa. Wszelkie systemy zbierające i przetwarzające dane są oparte na określonych algorytmach. Samo zbieranie i przetwarzanie danych nie stanowi problemu. Problemem jest podejmowanie na bazie tych danych określonych decyzji. Inteligencja systemów M2M jest ograniczona do określonej skończonej liczby przypadków, które zostały przez techników opracowane i wpisane jako możliwe scenariusze wyboru decyzji. System M2M „głupieje" często w przypadkach, które nie zostały ujęte (zaprogramowane wystarczająco jednoznacznie), a jak będzie reagował na zjawiska losowe, takie jak na przykład Tsunami, trzęsienia ziemi? Samo powiadomienie nie rozwiązuje problemu. Osobnym problemem są zjawiska błędnych decyzji systemów M2M wynikających ze złych algorytmów, które niedostatecznie zostały przetestowane.
- Zagrożenie wolności. Internet rzeczy podaje bardzo obszerną wiedzę o przepływach finansowych, zdrowiu, przyzwyczajeniach, preferencjach (zakupy przez

[14] Takie funkcje mają obecne na rynku opaski: FuelBand firmy Nike, Polor firmy Loop, Fitbit Flex, Samsung Gear Fit i dziesiątki innych. Opaski przypominają wyglądem zegarek. Mierzą aktywność fizyczną w ciągu dnia, gromadzą wszystkie informacje z treningu: zliczenie kroków, spalonych kalorii itp.

Internet, portale społecznościowe, oglądane strony www, programy telewizyjne i radiowe). Może to być wykorzystane w różny sposób przez osoby trzecie, które mają uprawniony (służby w USA mają dostęp do tych danych w ramach ustawy do walki z terroryzmem) bądź nieuprawniony dostęp do tych wrażliwych danych.

- Zagrożenie prywatności. W Internecie rzeczy zostawiamy pełną historię wszelakich operacji bankowych i tych realizowanych kartami. Wszystkie dane lokalizacyjne, miedzy innymi poprzez udostępnienie lokalizatora w telefonii komórkowej i wiele znaczników wskazujących na korzystanie ze sprzętu AGD, TV, samochodu, GPS, komputerów domowych i osobistych. Udostępnianie danych dotyczących tras podróży. A już odrębnym tematem jest historia naszych dolegliwości, zastosowanych procedur medycznych, zakupu leków itd. Poprzez odczyty mediów w naszych mieszkaniach, domach, dajemy pełną informację o liczbie osób przebywających w mieszkaniu, domu. Wszędzie, gdzie nasze dane stają się dostępne osobom trzecim, to zjawisko może mieć miejsce:
  - uruchomiona lokalizacja w telefonie;
  - dostęp poprzez TV i inne urządzenia domowe sterowane głosowo (wbudowany mikrofon) do treści wypowiadanych w pobliżu;
  - przedmioty ubieralne;
  - portale społecznościowe;
  - zakupy poprzez Internet i wynikające stąd preferencje zakupowe;
  - preferencje wynikające z przeglądania określonych stron www;
  - rozbudowana dostępność do danych medycznych, finansowych (np. BIK).
- Inne zagrożenia wolności i prywatności. Może ona sprowadzać się do pełnej inwigilacji związanej z systemami rozpoznawania twarzy. Tysiące kamer w sklepach, hotelach, mieście, na dworcach kolejowych i lotniczych, na drogach daje możliwość, poprzez system rozpoznawania twarzy, prześledzić historie naszych podróży, jak też śledzić nas online. Należy wspomnieć także o prostym, ogólnie dostępnym, oprogramowaniu przeszukiwania zdjęć w Internecie na podstawie zdjęcia twarzy. Zagrożenia wynikające z uprawnionych i nieuprawnionych (trudnych lub niemożliwych do weryfikacji) zastosowań wojskowych i policyjnych Internetu rzeczy[15]. W przypadku zgody na powszechne stosowanie osobistych RFID, nie będziemy mieli już sytuacji zagrożenia prywatności, tylko całkowite wyeliminowanie z dobrodziejstwem wszystkich możliwych zagrożeń, z wykluczeniem społecznym – na zamówienie – włącznie.

Podsumowanie

Spektrum zagrożeń o charakterze technicznym jest przeliczalne, ale praktycznie nieobliczalne. Można wskazać na kilka ważnych, wg autora, zagrożeń o charakterze technicznym:

- zagrożenia wynikające z niedostatecznego poziomu przetestowania konkretnego systemu. Można przyjąć założenie, że dynamika zmian w otoczeniu systemu,

[15] W maju W.W. Putin przekazał informację, że ze względu na układowo wmontowane oprogramowanie szpiegujące w systemie operacyjnym IOS i Android, po rewelacjach Edwarda Snowdena, Rosja przejdzie na system OS bazujący na fińskim oprogramowaniu SailFish.

może stworzyć zagrożenie, które wcześniej nie było znane (nie mówiąc o zwykłym nieujęciu wszystkich przypadków potencjalnych zachowań systemu);
- zagrożenie wynikające z awarii samego medium komunikacji, jakim jest Interent;
- zagrożenia wynikającego z wad technicznych stosowanych interfejsów i innych urządzeń peryferyjnych;
- zagrożenia wynikające z błędnych algorytmów, w tym algorytmów podejmowania decyzji;
- zagrożenie wynikające z braku standaryzacji oprogramowania[16], jego ogólnodostępnej możliwości aktualizacji. Mamy obecnie do czynienia ze zjawiskiem autorskich rozwiązań, których zabezpieczeniem przed kopiowaniem, kradzieżą jest między innymi brak otwartości i dostępu do oprogramowania (także zabezpieczanie oprogramowania układowe);
- zagrożenie wynikające z braku kompatybilności między oferowanymi systemami w obszarze sprzętowym, oprogramowania, jak i właściwości energonomicznych oferowanych systemów[17];
- zagrożenia wynikające z ograniczonej przestrzeni adresowej;
- zagrożenia wynikające z ograniczonej przepustowości Internetu;
- zagrożenia wynikające z zewnętrznej ingerencji osób trzecich w system, tak ukierunkowane na odniesienie konkretnych korzyści, jak i spowodowanie nie dających się przewidzieć innych zagrożeń, np. nieuprawnione wyłączenie prądu, gazu, wody do kłopotów z systemem zarządzania ruchem drogowym w mieście lub ruchem powietrznym na lotnisku.

---

[16] Brak standaryzacji oprogramowania niesie za sobą także pozytywne elementy związane z demonopolizacją rynku, omijaniem bardzo kosztownych opłat licencyjnych, tworzenie nowych innowacyjnych rozwiązań.

[17] Brak kompatybilności wynika z różnego podejścia do rozwiązania problemu i niesie za sobą także pozytywne elementy związane z demonopolizacją rynku, omijaniem bardzo kosztownych opłat licencyjnych, tworzenie nowych innowacyjnych rozwiązań.