Piotr Słowiński

NOWE METODY POPEŁNIANIA PRZESTĘPSTW NA PRZYKŁADZIE ROZWOJU INTERNETU RZECZY

Modern methods of commiting crime by the example of advancement of Internet of Things

Internet Rzeczy (ang. Internet of Things, dalej IR) jest definiowany w polskojęzycznych publikacjach jako koncepcja połączenia dwóch światów: wirtualnego i rzeczywistego, oparta na trzech filarach odnoszących się do cech inteligentnych obiektów: umożliwienia identyfikacji siebie nawzajem (wszystko jest w stanie się przedstawić), zapewnienia komunikacji (wszystko może się komunikować) i współdziałania (wszystko może wzajemnie na siebie oddziaływać)[1], można się również spotkać z pojęciem, że jest to swego rodzaju ekosystem, w którym wyposażone w sensory przedmioty komunikują się z komputerami[2]. Niezwykle istotna dla tej definicji jest koncepcja działania IR bazująca na trzech pojęciach: zawsze (*anytime*), wszędzie (*anyplace*) i ze wszystkim (*anything*)[3]. Celem rozwoju tejże koncepcji jest rozbudowanie, a właściwie zdominowanie komunikacji między urządzeniami elektronicznymi przez komunikację typu Maszyna–Maszyna (M2M). Obecnie IR jest przedmiotem badań głównie z punktu widzenia gospodarki i ekonomii, jako cecha mająca wzbogacić ofertę producentów tegu typu sprzętów, co w konsekwencji ma przełożyć się na lepsze wyniki sprzedaży. Niewłaściwemu rozumieniu tej koncepcji oraz zagrożeń z niej wynikających nie sprzyja również brak jednolitego nazewnictwa w polskojęzycznych publikacjach. Używane są głównie trzy określenia: Internet rzeczy, Internet przedmiotów czy angielska nazwa Internet of Things. Najlepszym postulatem byłoby przyjęcie jednej nazwy, mianowicie najbardzej logiczne wydawałoby się stosowanie odnoszącego się do nazwy angielskiej określenia Internet Rzeczy (zapisywanego w ten sposób). Ponadto niezbędne jest skonstruowanie odpowiedniej definicji IR, szczególnie na potrzeby kryminalistyki i rozważań podjętych w niniejszym tekście. Odpowiednia definicja obejmująca wszystkie problemy, z którymi można się spotkać w tym zakresie, mogłaby brzmieć następująco: Internet Rzeczy to koncepcja, w której większość lub wszystkie rzeczy codziennego użytku

[1] A. Brachman, *Internet przedmiotów – Raport*, Obserwatorium ICT, Technopark Gliwice 2013.

[2] *Raport Internet Rzeczy w Polsce*, IAB Polska, 2015.

[3] A. Brachman, op.cit.

lub po prostu rzeczy, których używamy, są połączone z Internetem i mogą zostać indywidualnie zidentyfikowane przez inne urządzenia bez aktywności człowieka. Występuje ona w postaci jednej wielkiej sieci powiązanych wzajemnie obiektów, komunikujących się ze sobą, wymieniających i zbierających dane. Dopiero tak skonstruowana definicja pozwala na odpowiednie zrozumienie zagrożeń oraz potencjalnej problematyki kryminalistycznej wynikających z rozwoju IR. Niniejsza publikacja ma na celu przybliżenie zarówno samego sposobu działania tej koncepcji, jak i zapoznanie z nowymi sposobami popełniania „klasycznych" przestępstw takich jak stalking, zabójstwo czy kradzież. Koncepcja ta występuje dopiero od niedawna w kontekście zagrożeń związanych z przestępczością, dlatego brak jest spraw, w których stałaby się ona narzędziem zbrodni. Z tego powodu poniższa praca będzie oparta w głównej mierze na rozważaniach teoretycznych, popartych eksperymentami przeprowadzanymi przez ekspertów ds. cyberbezpieczeństwa.

W celu lepszego zrozumienia IR należy przytoczyć krótką, lecz intensywną historię rozwoju tejże koncepcji. Przyjmuje się obecnie, że twórcą pojęcia Internet Rzeczy jest Kevin Ashton, który sformułował je już w 1999 r. i wróżył, że okaże się ono jeszcze większą rewolucją niż sam Internet. Jednak zwiększone zainteresowanie tą koncepcją zaczęło się dopiero wiele lat później, na co zwraca uwagę sam Kevin Ashton.[4] Skupiono się głównie na możliwym zastosowaniu jej w rozwoju technologicznym w celu ułatwienia codziennego życia, skoncentrowano się więc raczej na biznesowym wykorzystaniu tej nowatorskiej i interesującej koncepcji. Już w 2010 r. do urządzeń łączących się bezprzewodowo można było zaliczyć wiele przedmiotów m.in. lodówki, mikrofalówki, zegary, kuchenki, ekspresy do kawy, naturalnie komputery wraz z wszelkimi towarzyszącymi im urządzeniami oraz telefony komórkowe. W roku 2015 do urządzeń, do których odnosi się koncepcja IR, możemy zaliczyć nie tylko powyższe przedmioty, ale również: sprzęt medyczny, wszelkiego rodzaju czujniki i systemy monitorowania, np. stanu zdrowia czy lokalizujące zwierzęta, przedmioty używane do uprawiania sportu, akcesoria rowerowe, samochodowe lub ogrodowe – właściwie wszystkie, w których można umieścić modem sieci bezprzewodowej, pozwalający łączyć się dzięki niej z innymi przedmiotami. Według informacji zamieszczonej w prezentacji stworzonej wspólnie przez naukowców z University College London i brytyjskiego Home Office, do 2020 r. liczba urządzeń połączonych ze sobą może wynieść 25 miliardów, co jest uważane za wyliczenie bardzo ostrożne: prawdopodobnie będzie ona większa.[5]

Obiekty mieszczące się w ramach koncepcji IR są tak różnorodne, że nie sposób je zaklasyfikować w jedną ścisłą grupę; można je jedynie ogólnie określić jako „przedmioty codziennego użytku" bądź jeszcze bardziej ogólnie: „przedmioty, których używamy". Słowo „Internet" wiele osób do tej pory wiąże jedynie z komputerami bądź ewentualnie z telefonami komórkowymi czy tabletami. W tym miejscu pojawia się już pierwsze z zagrożeń – niewiedza. Ludzie nie zdają sobie sprawy,

[4] http://www.rfidjournal.com/articles/view?4986, [22.06.2009].

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf, [10.03.2015].

że tak naprawdę obecny kierunek rozwoju powoduje, iż w funkcję bezprzewodowego łączenia się z Internetem bywają wyposażone takie przedmioty jak lodówki, czajniki, zabawki, bramy garażowe, samochody oraz wiele innych podobnych. Co ważne, obiekty te łączą się ze sobą np. poprzez jedno konto, uzyskują dostęp do innych urządzeń powiązanych tym kontem lub po prostu będących połączonych z tym samym modemem Wi-Fi. Do tej pory Internet Rzeczy utożsamiany był często z nieuchronnym rozwojem technologicznym prowadzącym do przekształcenia przeciętnego domu, w tzw. smartdom, co miało być znaczącym ułatwieniem w życiu. Niewiele osób dostrzegało w tym potencjalne zagrożenie, co ważniejsze, nie dostrzegali tego również producenci takich rozwiązań. Nie wyposażali swoich produktów w odpowiednie zabezpieczenia, mogące ochronić użytkowników przed niepożądanymi działaniami osób trzecich. Rozwiązania mające być częściami składowymi takich systemów nie były w odpowiedni sposób testowane, m.in. pod kątem zagrożeń związanych z atakami hakerskimi. Internet Rzeczy nie może być jednak postrzegany tylko jako produkt, który da się sprzedać. Ścisłe powiązanie życia rzeczywistego i wirtualnego powoduje, że po stronie producentów oprócz zysków powinno się pojawić równie wysokie poczucie odpowiedzialności za bezpieczeństwo osób korzystających z tych rozwiązań. Na podstawie przykładów i eksperymentów można wysnuć wnioski co do kierunku rozwoju IR i problemów powstających z punktu widzenia kryminalistyki i szerzej prawa, a konkretnie nowych metod dokonywania przestępstw i wykrywania sprawców. Niektóre z przedstawionych w poniższym tekście przykładów mogą nie mieć zastosowania do wszystkich typów przestępstw, jednak celem tego artykułu jest ukazanie jak wiele istnieje potencjalnych szans wykorzystania IR do popełniania różnego typu czynów zabronionych.

Posługując się terminologią z dziedziny prawa karnego, a mianowicie pojęciem iter delicti, czy właściwie bardziej adekwatnym pojęciem form stadialnych przestępstwa, zastosowanie IR można zauważyć już na etapie przygotowania do popełnienia czynu zabronionego. Ciekawa pod tym względem będzie sytuacja z sierpnia 2015 r., kiedy badacze bezpieczeństwa z firmy Pen Test Partners „zhakowali" „smartlodówkę" firmy Samsung. Lodówka ta synchronizuje się z kalendarzem Gmail i pozwala wyświetlać go na wbudowanym ekranie oraz dokonywać w nim zmian. Badacze odkryli, że urządzenie jest podatne na ataki typu Man-In-The-Middle. Lodówka używa certyfikatu bezpieczeństwa SSL, jednak nie jest w stanie go w odpowiedni sposób uwierzytelnić. Umożliwia to hakerowi dostęp do konta Google użytkownika lodówki dzięki połączeniu się z siecią, z którą ta lodówka również jest połączona. Po doniesieniach prasowych oraz informacjach uzyskanych od firmy Pen Test Partners firma Samsung zajęła się wyjaśnianiem błędu w oprogramowaniu i oczywiście obiecała go rozwiązać. Wykorzystanie powyżej opisanej luki przez potencjalnego sprawcę wydaje się naturalne – uzyskuje on dostęp do planu dnia, ważnych danych wrażliwych lub innych istotnych informacji dotyczących ofiary, co w oczywisty sposób pozwala mu zaplanować przestępstwo. Taki atak otwiera perspektywę uzyskania dostępu do danych często nieosiągalnych w inny sposób, np. danych osoby, która strzeże swojej prywatności na portalach społecznościowych, prowadzącej często życie prywatne

i zawodowe za pośrednictwem konta mailowego, albo pozwala na poznanie haseł i numerów kont bankowych. Kolejną niepokojącą kwestią umożliwiającą obserwację potencjalnej ofiary jest uzyskanie dostępu do kamer monitoringu tzw. CCTV (ang. Closed Circuit TeleVision). Prywatne kamery często nie mają odpowiednich zabezpieczeń uniemożliwiających włamanie do nich, a coraz częściej zdarza się że są połączone z Internetem. Brak zabezpieczeń może wynikać albo z braków w oprogramowaniu, albo z zaniedbania samych użytkowników, np. z tego, że domyślne hasło nie zostanie zmienione. O skali problemu niezabezpieczonych kamer może świadczyć strona www.insecam.org, na której można uzyskać podgląd obrazu z takich kamer, znajdujących się w różnych krajach. Kolejnym niepokojącym sygnałem związanym właśnie z kamerami czy szerzej pojętym sprzętem do nagrywania obrazu i dźwięku są doniesienia z końca 2015 r. oraz ze stycznia i czerwca 2016 r. dotyczące możliwości dokonania ataków hakerskich za pośrednictwem lalki Barbie i tzw. elektronicznej niani (ang. baby monitor). Pierwsze doniesienie dotyczyło tego, że lalka Hello Barbie, która ma funkcje łączenia się z Internetem i umożliwia dziecku „rozmowę" z nią, wykazywała podatność na atak ze względu na słabości w oprogramowaniu, co pozwalało hakerom na zamianę aplikacji sterującej lalką zainstalowaną na telefonach z systemami iOS lub Android. Dzięki zamianie atakujący mógł uzyskać dostęp do haseł i innych poufnych informacji, ponadto aplikacja łączyła się z każdą siecią ze słowem „Barbie" w nazwie, co umożliwiłoby stworzenie przez sprawcę ataku fałszywej sieci do przechwytywania całej wymiany danych prowadzonej z takiego telefonu[6]. Doniesienia ze stycznia i czerwca 2016 r. dotyczą natomiast podatności na ataki urządzeń służących rodzicom do obserwowania dzieci, np. w trakcie snu, czyli tzw. elektronicznych niań. Zagrożenie atakiem było duże, szczególnie gdy urządzenia nie miały haseł lub te hasła nie były zmieniane w ogóle lub od dawna. Dokonujący ataków mogli mówić do dzieci za pośrednictwem tych urządzeń, a jeśli zostały one wyposażone w kamerę to mogli też widzieć dziecko[7]. Jeszcze jednym bardzo interesującym przykładem, który może wzbudzać zaniepokojenie oraz świadczyć o skali problemu niezabezpieczonych przedmiotów z dostępem do Internetu, jest eksperyment amerykańskiej firmy Praetorian, która skonstruowała drona wyposażonego w specjalny wykrywacz urządzeń i przedmiotów z dostępem do sieci Wi-Fi. W ciągu 18–minutowego lotu nad Austin w stanie Teksas dron ujawnił ponad 1600 takich urządzeń[8]. Taka sytuacja była możliwa, ponieważ obecnie większość przedmiotów, do których ma zastosowanie koncepcja IR, korzysta z jednego rodzaju systemu komunikacji bezprzewodowej pod nazwą ZigBee. Komunikacja między urządzeniami

[6] http://www.pcworld.com/article/3012220/security/internet-connected-hello-barbie--doll-can-be-hacked.html, [07.12.2015].

[7] http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked--parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html, [30.01.2016]; http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/, [04.08.2016].

[8] http://thehackernews.com/2015/08/hacking-internet-of-things-drone.html, [07.08.2015]; https://www.praetorian.com/iotmap/#15/30.2647/-97.7520, [2015].

odbywa się na poziomie w miarę otwartym i każde z nich wysyła swego rodzaju sygnał w celu połączenia się z innymi. Właśnie to wykorzystali badacze, uzykując wspomniane wyniki doświadczenia. Powyższe przykłady stanowią jedynie papierek lakmusowy możliwości wykorzystania niektórych elementów koncepcji IR do przygotowania popełnienia przestępstwa. Słabość systemów, a konkretnie ich zabezpieczeń, jest niezwykle groźna już na etapie pozyskiwania danych o potencjalnej ofierze. Naturalnie powyższe przykłady mogą być wykorzystane do dokonania przestępstwa np. kradzieży tożsamości, kradzieży z włamaniem czy też innego typu podobnych przestępstw, a nie tylko ich przygotowania.

Po krótkim omówieniu możliwości wykorzystania Internetu Rzeczy do formy stadialnej przygotowania, można przejść do bardziej rozbudowanej, a przez to dalece bardziej interesującej formy stadialnej, czyli dokonania. W tym aspekcie IR oferuje ogromne spektrum możliwości, prawie że nieograniczone niczym poza wyobraźnią potencjalnego sprawcy przestępstwa. Pierwszym przytoczonym przykładem, chyba najbardziej niepokojącym, będzie eksperyment dotyczący przejęcia przez hakerów kontroli nad samochodem marki Jeep. Przeprowadzili go dwaj specjaliści od zabezpieczeń, Charlie Miller i Chris Valasek dla magazynu WIRED[9]. Dokonali ataku na Jeepa Cherokee prowadzonego przez dziennikarza WIRED na drodze międzystanowej. Co istotne, atak odbył się przez Internet z domu oddalonego o kilka kilometrów. Wcześniejszy eksperyment obu badaczy został przeprowadzony na tym samym dziennikarzu w roku 2013. Wtedy „sprawcy" musieli siedzieć w tym samym samochodzie co ich „ofiara", ponieważ atak na systemy elektroniczne samochodu był możliwy jedynie po podłączeniu komputera do samochodu przez port wykorzystywany przez mechaników w trakcie przeglądów technicznych. Rok przygotowań pozwolił na rozwinięcie tej metody na tyle, że umożliwił atak na nowy samochód (rocznik 2014) bez konieczności przebywania w nim. Eksperyment zaczął się od manipulowania klimatyzacją, następnie Miller i Valasek włączyli głośną muzykę (niedającą się przyciszyć) i wyświetlili na ekranie w samochodzie swoje zdjęcie-podpis. Kolejnym działaniem było między innymi włączenie wycieraczek i spryskiwaczy, tak intensywne, że uniemożliwiało obserwację drogi przed kierowcą. Ostatecznym działaniem było „zabicie" silnika – zablokowanie pedału przyspieszania i zwolnienie samochodu do bardzo niskiej prędkości. Wszystko to przy akompaniamencie ogłuszającej muzyki. Pełnię możliwości przygotowanego przez nich planu badacze zaprezentowali później na parkingu – przy niskiej prędkości atakujący systemy elektroniczne pojazdu może całkowicie wyłączyć silnik, włączyć hamulce lub je wyłączyć oraz – choć tej czynności jeszcze do końca nie dopracowano, przejąć kontrolę nad kołami. Oczywiście jest też w stanie dokładnie zlokalizować dany samochód dzięki systemowi GPS. Tego typu atak jest możliwy, ponieważ coraz więcej producentów samochodów implementuje do nowych modeli jak najwięcej systemów elektronicznych, w teorii mających ułatwić użytkownikowi korzystanie z samochodu oraz umożliwić producentowi monitoring zużycia poszczególnych części w trakcie eksploatacji. W praktyce firmy samochodowe nie zabezpieczają elektronicznych systemów pojazdów w odpowiedni sposób przed zewnętrznymi atakami, stwarzając tym samym

[9] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, [21.07.2015].

okazję do wykorzystania takich luk przez przestępców. Kontrolę nad samochodem można uzyskać z jakiekolwiek miejsca, pod warunkiem że zna się jego adres IP, co dla hakera nie jest szczególnie skomplikowane. Jakkolwiek eksperyment może z zewnątrz wydawać się zabawny, to sam dziennikarz, choć był przygotowany na fakt, że coś z samochodem się będzie dziać, opisywał swoje przeżycia jako autentyczny strach o własne bezpieczeństwo. Można tylko sobie wyobrazić strach i panikę osoby, która nie byłaby przygotowana na taki atak. Po opisaniu przebiegu doświadczenia należy w skrócie wyjaśnić, dlaczego jest on możliwy i co tak właściwie zostało zaatakowane. Współczesne samochody są wyposażane w coraz większą liczbę komputerów, występujących w postaci tzw. ECU (ang. electronic control unit). Są one odpowiedzialne za takie działania jak np. monitoring ciśnienia powietrza w oponach, nawigacja samochodowa, kontrola oświetlenia samochodowego oraz właściwie wszystkie elektroniczne czujniki zużycia poszczególnych komponentów pojazdu, a także obecnie coraz częściej za jego przyspieszanie, hamowanie i kontrolę prędkości. Dobrym podsumowaniem skuteczności eksperymentu, jak i podatności samochodów na ataki oraz skali zagrożenia, niech będzie informacja, że po tym eksperymencie firma Chrysler (wytwórca samochodów marki Jeep) wycofała z rynku 1,4 miliona aut. O powadze zagrożenia może również świadczyć fakt, że zwróciło ono uwagę nie tylko mediów, lecz także FBI, które w swoim komunikacie z 17 marca 2016 r.[10] odniosło się do możliwości ataku na systemy elektroniczne samochodu, takiego jak opisany powyżej. W komunikacie służby zwracają zarówno producentom samochodów oraz części samochodowych, jak również konsumentom uwagę na podatność komponentów elektronicznych na ataki, w sytuacjach gdy nie będą one w odpowiedni sposób zabezpieczone. FBI dostrzegło również bardzo interesujące zjawisko, związane z IR. Wspomina mianowicie o częściach i urządzeniach dodatkowych, nie występujących fabrycznie w samochodach, ale które można kupić oddzielnie i dołączyć do pojazdu i które następnie funkcjonują tak jak fabryczne ECU. Jednym z przykładów wykorzystania w taki sposób zwykłych gadżetów samochodowych, kupowanych często przez samych użytkowników, jest urządzenie francuskiej firmy Mobile Devices nazwane OBD2. Gadżet ten podłączany był do deski rozdzielczej i miał służyć jednej z firm startupowych do kontroli lokalizacji pojazdów i liczby kilometrów pokonanych przez klienta. Badacze z Uniwersytetu Kalifornijskiego w San Diego (UCSD) na przykładzie Corvetty z 2013 r. udowodnili, że można przejąć kontrolę nad tymi urządzeniami i w konsekwencji wysyłać pewne komendy, które mają wpływ na działanie ECU samochodu. Dokonali tego poprzez wysyłanie odpowiednio napisanych wiadomości SMS, w których umieścili komendy trafiające do magistrali CAN (wewnętrznej sieci pozwalającej kontrolować fizyczne elementy samochodu). Naukowcy byli w stanie włączyć wycieraczki oraz sprawić, że hamulce zadziałają lub przestaną działać. Kierownik zespołu badaczy Stefan Savage twierdził nawet, że dzięki tym małym gadżetom można by przejąć kontrolę praktycznie nad wszystkimi elektronicznymi elementami samochodu[11].

[10] https://www.ic3.gov/media/2016/160317.aspx, [17.03.2016].

[11] https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/, [11.08.2015].

Bardzo niepokojącą metodą dokonania przestępstwa są badania dotyczące karabinu snajperskiego z systemem wspomagającym celowanie TrackingPoint. Jego celem jest zautomatyzowanie celowania, w taki sposób, że to system ma decydować, kiedy karabin znajduje się w odpowiedniej pozycji do oddania strzału, ograniczając rolę strzelca jedynie do pociągnięcia za spust. Badacze zabezpieczeń Runa Sandvik oraz Michael Auger wykazali, że system ten jest podatny na ataki, m.in. ze względu na możliwość włączenia fabrycznie zablokowanego Wi-Fi oraz na braki w oprogramowaniu. W toku eksperymentu ustalili, że haker może, przy włączonym Wi-Fi, dokonywać zmian w parametrach celowania karabinu, zablokować spust lub nawet cały karabin[12]. Z punktu widzenia możliwości popełnienia przestępstwa należy się szczególnie skupić na tym pierwszym. Jak wynika z doświadczenia Sandvik i Augera, zmiana wagi pocisku w tym programie na większą powoduje, że uderzy on w cel znajdujący się po lewej stronie od tego wybranego przez strzelca, natomiast wprowadzenie mniejszej niż rzeczywista lub ujemnej wagi pocisku spowoduje odchył w prawo. W ten sposób haker może zmienić cel bez wiedzy strzelca, znajdując się od niego w odległości umożliwiającej połączenie się z systemem TrackingPoint. Choć na razie znalezienie takiej luki w zabezpieczeniach wymagało rozebrania jednego z dwóch karabinów znajdujących się w posiadaniu badaczy, to niepokojący może się wydawać fakt, że producent tych systemów nie zadbał o bezpieczeństwo w stopniu chociażby bardzo utrudniającym atak na sprzedawane przez siebie urządzenie. Naturalnie producent po ukazaniu się reportażu w magazynie WIRED obiecał zająć się tą sprawą i dostarczyć użytkownikom aktualizację mającą zaradzić problemom wykrytym przez badaczy. Dziwny i szokujący może się wydać fakt, że Sandvik i Auger kontaktowali się już wcześniej w tej sprawie z tymże producentem, oferując mu dodatkowo pomoc w naprawieniu wykrytych przez nich problemów. Nie doczekali się jednak odpowiedzi pomimo wielu prób skontaktowania się z przedstawicielami firmy. Na szczęście problem karabinów dotyczy jedynie nieco ponad 1000 sztuk, bo tyle do wykonania eksperymentu udało się tej firmie sprzedać od 2011 r. Jednak to, co szczególnie powinno niepokoić, m. in. ze względu na możliwość wykorzystania tego typu narzędzi do popełnienia przestępstwa zabójstwa, to fakt, że wraz z rozwojem koncepcji IR pojawiać się będzie coraz więcej przedmiotów z przedrostkiem „smart-", również tych które niosą za sobą realne zagrożenie dla zdrowia i życia nie tylko konsumentów z nich korzystających, ale również dla innych, postronnych osób.

Trzecim, zdawałoby się najbardziej przerażającym sposobem jest zhakowanie sprzętu medycznego w postaci dozowników leków oraz rozruszników serca. Specjalista od zabezpieczeń Billy Rios w 2015 r. przeprowadził dwa eksperymenty, badając dozowniki leków w szpitalach[13]. W pierwszym chciał zbadać, czy istnieje możliwość dokonania ataku na takie urządzenie i zmiany dawki leku podawanego pacjentowi. Udało mu się to, jednak nie mógł zwiększyć dawki leku dowolnie bez wszczynania

[12] https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/, [29.07.2015].

[13] https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/, [08.06.2015].

alarmu, jedynie w ramach zaprogramowanych fabrycznie limitów. W drugim ataku, przeprowadzonym w czerwcu 2015 r., jak twierdził w relacji dla magazynu WIRED, udało mu się podmienić biblioteki plików, zawierające odpowiednie limity dla każdego z leków, na własne, z dawkami przekraczającymi maksymalne dopuszczane. Rios wykazał również, że utrudnieniem dla hakera byłoby, gdyby sprzęt tego typu akceptował jedynie aktualizacje cyfrowo podpisane odpowiednim certyfikatem bezpieczeństwa. W przypadku sprzętu, na którym przeprowadzał eksperyment, okazało się jednak, że akceptuje on wszystkie aktualizacje, a więc również te odpowiednio „spreparowane", przykładowo przez hakera. Taka „aktualizacja" pozwala hakerowi nie tylko na zmianę dawki na niebezpieczną dla zdrowia i życia, ale również na wyświetlanie na ekranie dozownika błędnych informacji, jakoby podawana była odpowiednia dawka. Firma, na której urządzeniach badacz testował podatność na ataki, cały czas twierdzi, że zaatakowane systemy są od siebie w odpowiedni sposób fizycznie odseparowane. Elementy sprzętu są rzeczywiście fizycznie oddzielone, poza jednym kablem, co według Riosa umożliwia przeprowadzenie opisanego przez niego ataku. Twierdzi on ponadto, że atakujący nie potrzebuje mieć fizycznego dostępu do dozownika, ponieważ ataku można dokonać przez Internet, po podłączeniu się do szpitalnych sieci. Producent urządzeń potwierdza, że dozowniki leków mają połączenia z Internetem pośrednio dzięki połączeniu ze szpitalnymi sieciami, ponieważ w ten sposób firma dokonuje aktualizacji oprogramowania. Zdaniem producenta nie ma to wpływu na bezpieczeństwo urządzeń i ze względu na wspomniane już odseparowanie tych elementów atak opisywany przez Riosa nie jest możliwy do przeprowadzenia.

Kolejną niebezpieczną metodą wydaje się możliwość ataku na rozrusznik serca. Do niedawna mogło to wydawać się możliwe jedynie w filmach (atak tego typu został pokazany w serialu Homeland), lecz eksperyment przeprowadzony przez studentów z University of South Alabama (USA) na bardzo zaawansowanym fantomie szkoleniowym dla studentów medycyny zwanym iStan udowodnił, że nie jest to tylko wizja artystyczna twórców seriali[14]. Obiekt doświadczenia charakteryzuje się tym, że jest najbardziej realistycznym fantomem o zachowaniach zbliżonych do człowieka – płacze, mówi, poci się, reaguje na 300 różnych leków w taki sam sposób jak organizm ludzki. Jest również wyposażony w rozrusznik serca do sterowania pracą jego mechanicznego odpowiednika, i to właśnie on stał się celem ambitnych studentów USA, którzy chcieli sprawdzić podatność rozrusznika na atak hakerski. W toku eksperymentu okazało się, że studenci mogli w dowolny sposób zmieniać tętno i gdyby rozrusznik był wyposażony w defibrylator, byliby w stanie wpływać na tętno poprzez kontrolowane wstrząsy. Podatność takich urządzeń jak rozruszniki na zhackowanie wynika z tego, że są one wyposażone w łączność bezprzewodową z Internetem. Celem było to, aby lekarz mógł obserwować stan pacjenta w czasie rzeczywistym, niekoniecznie zapraszając go na wizytę, lub w razie sytuacji awaryjnej uratować mu życie. Małe rozmiary rozruszników powodują, że nie są one wyposażone w odpowiednie zabezpieczenia, które szyfrowałyby te bezprzewodowe połączenia. Ten fakt również stał się polem badań

[14] http://motherboard.vice.com/read/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker, [07.09.2015].

studentów USA – pracują nad rozwiązaniem problemu i opracowaniem odpowiedniego szyfrowania. O powadze i randze zagrożenia może świadczyć wywiad udzielony stacji CBS przez byłego wiceprezydenta Dicka Cheneya, posiadacza tego typu rozrusznika[15]. Poinformował w nim, że w obawie przed możliwym atakiem hakerskim zwrócił się do lekarzy z prośbą o wyłączenie funkcji bezprzewodowych w swoim urządzeniu na czas sprawowania przez niego urzędu. Należy wziąć pod uwagę, że było to na jakiś czas przed zarówno wspomnianym eksperymentem studentów, jak i emisją serialu. Obecnie pojawia się wiele głosów, zarówno pojedynczych osób, jak i agencji federalnych, że zagrożenie w związku z atakiem na tego typu urządzenia nie jest powszechne. Nie można jednak zapominać, że w związku z szybkim rozwojem technicznym mogą się pojawić kolejne tego typu niebezpieczeństwa, m.in. w konsekwencji wyposażania sprzętu medycznego w funkcje bezprzewodowe.

Niezwykle groźnym sygnałem wskazującym na niebezpieczeństwa, których ofiarą może w przyszłości paść każdy człowiek, jest podatność urządzeń będących częścią IR na zhakowanie, połączona z rozpowszechnieniem takich systemów i przedmiotów w naszym codziennym życiu, w postaci koncepcji już wspomnianej wyżej, a mianowicie tzw. smartdomu, czyli domu, w którym większość lub prawie wszystkie systemy będą mogły być sterowane przykładowo za pośrednictwem aplikacji na telefonie. Mowa tu o systemach odpowiedzialnych za ogrzewanie, oświetlenie, bramy garażowe, alarmy antywłamaniowe aż po sterowanie zamkami drzwi. Próbę zaatakowania systemów zarządzających poszczególnymi elementami tzw. smartdomu podjęło dwóch badaczy z firmy Cognosec – Tobias Zillner i Sebastian Strobl[16]. Jak wskazali w swoim badaniu, producenci powyższych systemów opierają ich działanie na wspomnianym już w tym tekście systemie ZigBee, najbardziej popularnym wśród urządzeń będących częścią IR. System ten jest skonstruowany tak, żeby działał jak najprościej – ma być prosty w konfiguracji, tani w produkcji oraz nie pobierać dużo energii, co musi odbijać się na możliwościach zaimplementowania w nim narzędzi służacych do lepszego jego zabezpieczenia. Sposób ataku jest niezwykle prosty – trzba zakłócić działanie sensora, a ze względu na jego nieskomplikowaną budowę, wystarcza do tego sygnał dźwiękowy. Powoduje to, że urządzenie sterujące nie może się połączyć z kanałem ZigBee. Statystycznie większość użytkowników po zauważeniu takiej sytuacji dokonuje najprostszej czynności w celu przywrócenia połączenia, mianowicie resynchronizacji urządzenia i sieci ZigBee, czyli wysłania jeszcze raz klucza sieciowego. To pozwala atakującemu na przechwycenie go, a przez to uzyskanie pełnej kontroli nad systemem, ponieważ całe zabezpieczenie oparte jest na tym kluczu. Ponadto w toku badań nie stwierdzono, aby system był w stanie zmienić lub zresetować klucz, zarówno manualnie, jak i automatycznie. Z tego powodu nawet jeśli użytkownik zorientuje się, że w jego sieci znajduje się osoba niepożądana lub jest on obiektem niepożądanych działań, to nie jest w stanie nic z tym zrobić. W wyniku eksperymentu badacze zdołali przejąć kontrolę nad

[15] http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434, [19.10.2013].

[16] https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good--The-Bad-And-The-Ugly-wp.pdf, [06.08.2015].

urządzeniami podłączonymi do tego systemu, m.in. oświetleniem w domu, systemem alarmowym oraz nad zamkami w drzwiach. Najbardziej niepokojący jest jednak fakt, na co zwrócili uwagę również wspomniani badacze, że użytkownik takiego systemu nie jest w stanie nawet się odpowiednio zabezpieczyć, chociażby wykrył, że stał się ofiarą ataku hakerskiego. Bezsilność wynika głównie z ograniczeń sprzętowych, które, jak już wcześniej wspomniano, mają być proste w obsłudze, a przez to są mało wyrafinowane pod względem zabezpieczeń. W tym wypadku konsumenci muszą polegać na producentach, którzy powinni wdrożyć lepsze zabezpieczenia lub zapewnić odpowiednie aktualizacje oprogramowania, uniemożliwiające takie sytuacje jak opisana powyżej.

Powyższe przykłady, dotyczące wykorzystania IR zarówno do przygotowania, jak i dokonania przestępstwa, często można było odnieść jedynie do pojedynczych ofiar. Jednak wraz z rozwojem IR i postępującą automatyzacją właściwie wszystkich elementów zarządzanych elektronicznie wprost proporcjonalnie zwiększa się też zagrożenie dla znacznej liczby ludzi. Mowa tu o systemach elektronicznych wykorzystywanych w zarządzaniu miastem oraz infrastrukturze krytycznej. Coraz więcej miast wprowadza automatyzację sygnalizatorów świetlnych, systemów zarządzających oświetleniem, wodą i energią oraz bezpieczeństwem, np. miejskiego monitoringu. Postęp ten dokonuje się obecnie coraz szybciej, coraz więcej miast decyduje się na rozwój w tym właśnie kierunku i dzieje się tak z wielu względów – np. ekonomicznych lub logistycznych. Podobnie jednak jak w przypadku rzeczy codziennego użytku, również te systemy powinny mieć odpowiednie zabezpieczenia, i to każdy z ich elementów. Wystarczy jeden słaby punkt, aby doświadczony haker wykorzystał lukę w zabezpieczeniach, co w konsekwencji stanowiłoby być może zagrożenie nawet dla całej populacji miasta. Wspomniane wyżej systemy automatyczne działają często w oparciu o system SCADA (ang. Supervisory Control And Data Acquisition), który ma za zadanie zbierać pomiary, wizualizować je, sterować działaniami podłączonych urządzeń oraz archiwizować dane i wykrywać ewentualne nieprawidłowości. Przykładowo system ten może kontrolować ciśnienie na zaworach w miejskim przedsiębiorstwie wodociągowym czy też monitorować przepływ prądu w miejskiej elektrowni. Jeśli częściami systemu elektronicznego zarządzania miastem będą łatwe do zhakowania obiekty należące do koncepcji IR, to może to spowodować bardzo poważne zagrożenie. Uzyskanie przez potencjalnych sprawców dostępu do oprogramowania zarządzającego infrastrukturą krytyczną może w najlepszym przypadku skończyć się paraliżem miasta, a w gorszych scenariuszach dokonaniem np. przestępstwa o charakterze terrorystycznym o skali zniszczeń nieporównywalnie większej niż popełnionego w jednym miejscu, np. z użyciem jednego dużego ładunku wybuchowego. Obecnie zagrożenie atakiem terrorystycznym na tak dużą skalę, jak atak na całe miasto przy użyciu IR oraz szerzej, systemów elektronicznego zarządzania miastem, którego celem byłaby infrastruktura krytyczna, wydaje się odległy, głównie ze względu na koszty i trudności organizacyjne, wynikające ze skali i trudności takiego ataku. W momencie pisania tego tekstu brak jest organizacji terrorystycznych zdolnych do przeprowadzenia zakrojonej na tak szeroką skalę akcji. Nie można jednak wykluczyć, że w przyszłości, być może nawet niedalekiej, taka grupa powstanie i będzie zdolna do dokonania tego typu przestępstwa. Ataki na system SCADA

nie są powszechne, jednak historia już zna takie przypadki. Te najbardziej znane to wirus Stuxnet mający powstrzymać rozwój irańskiego programu nuklearnego[17] czy też ostatnie wydarzenia z grudnia 2015 r. na Ukrainie[18], gdzie wirus BlackEnergy Trojan spowodował, że system SCADA w punktach przesyłowych jednej z firm energetycznych przestał działać, co doprowadziło do tego, że w tysiącach domów zabrakło prądu[19].

Sytuacje przedstawione w powyższym tekście miały na celu wskazanie na możliwe zagrożenia, jakie wynikają z rozwoju koncepcji Internetu Rzeczy, i zwrócenie uwagi na problemy, jakie mogą się pojawić, jeśli tę koncepcję zechcą wykorzystać przestępcy do przygotowywania i dokonywania przestępstw. Celem było również ukazanie problematyki kryminalistycznej rozwoju tej techonologii – pojawienie się nowych sposobów dokonywania przestępstw, wykorzystanie przestrzeni wirtualnej do popełniania przestępstw jak najbardziej „realnych". Tekst ten powstał również, aby spróbować zdefiniować pojęcie Internetu Rzeczu na potrzeby kryminalistyki, podsumować i zsyntetyzować stan wiedzy o zagrożeniach wynikających z wykorzystania IR do popełniania przestępstw, również ze względu na to, że brak jest właściwie literatury na ten temat. Z polskich publikacji godnym polecenia tekstem, który może posłużyć jako wstęp do zrozumienia, czym jest IR i jak funkcjonuje, jest artykuł Macieja Kołodzieja w pokonferencyjnej publikacji, wydanej przez Wyższą Szkołę Policji w Szczytnie[20]. W momencie pisania tego tekstu w obiegu dostępna jest publikacja dotycząca bezpieczeństwa w „smart-miastach" związanego z koncepcją IoT[21]. Za granicą godnym pochwalenia posunięciem jest stworzenie przez brytyjskie Home Office (odpowiednik polskiego MSW) wspólnie z naukowcami z University College London prezentacji traktującej ściśle o zagrożeniach wynikających z korzystania z przedmiotów połączonych z Internetem[22]. Cel i wizja przyszłości, w której IR jest częścią otaczającej wszystkich ludzi rzeczywistości, został idealnie określony w artykule opublikowanym w magazynie WIRED w grudniu[23], niejako podsumowującym rok 2015 pod kątem rozwoju IR oraz pojawienia się eksperymentów wskazujących na zagrożenia bezpieczeństwa użytkowników. Cytat z tego tekstu: „There was once a time when people distinguished between cyberspace, the digital world of computers and hackers, and the flesh-and-blood reality known as meatspace". Rzeczywiście, jednak przyszłością jest koncepcja opisana w tym tekście, niezależnie od tego jak dużą przychylnością będziemy ją darzyć, jeśli w ogó-

[17] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, [03.11.2014].
[18] http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231, [31.12.2015].
[19] http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/, [04.01.2016].
[20] M. Kołodziej, *Internet Rzeczy, nowe spojrzenie na ochronę prywatności*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna 2015*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno 2015.
[21] G. Szpor (red.), *Internet rzeczy. Bezpieczeństwo w Smart City*, C.H. Beck, Warszawa 2015.
[22] Zob. przyp. 5.
[23] https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/, [28.12.2015].

le będziemy nią zainteresowani. Prędzej czy później „spotkamy" ją, czy to kupując nowy samochód, zmywarkę, lodówkę, telefon komórkowy, czy może budując nowy dom bądź urządzając mieszkanie. Internet Rzeczy będzie nam towarzyszył, ale to, co można zrobić, by nie paść ofiarą przestępstwa, do którego jako narzędzie zbrodni zostanie wykorzystana nasza lodówka lub samochód, to świadoma decyzja zakupu przedmiotów wyposażonych w funkcje bezprzewodowego łączenia się z Internetem. Ogromna rola w zwalczaniu tego rodzaju cyberprzestępczości leży również w rękach służb oraz organów ścigania oraz rządzących. Policja oraz inne organy zobowiązane do ścigania przestępstw nie mogą „pozostawać w tyle", muszą nadążać za rozwojem technologicznym, aby lepiej móc wypełniać swoje ustawowe zadania. Najlepiej, żeby ten rozwój rozpoczął się jak najwcześniej, zanim wydarzy się sytuacja, w której przestępcy wykorzystają IR do popełnienia przestępstwa. Jest to zresztą jeden z grzechów producentów sprzętów i urządzeń opisanych w tym tekście – pomimo sygnałów od badaczy zabezpieczeń zdarza się, że nie reagują na nie, dopóki sprawa nie zostanie opisana w gazetach lub nagłośniona w Internecie. Niezbędna jest też edukacja samych użytkowników takich urządzeń, swego rodzaju świadomość tego, co się kupuje i jak to działa, chociażby na poziomie ogólnym, i jakie ewentualne zagrożenia mogą się wiązać z używaniem tego typu sprzętu. W celu uchronienia się przed negatywnymi skutkami korzystania z urządzeń wchodzących w skład koncepcji Internetu Rzeczy nie jest konieczne, aby wyjechać np. w Bieszczady i zamieszkać z dala od cywilizacji. Najbardziej istotną, lecz również najbardziej oczywistą kwestią jest myślenie nie tylko o korzyściach, ale również o zagrożeniach, jakie niesie ze sobą automatyzowanie naszego życia i rzeczy, których używamy.

Streszczenie

Artykuł podejmuje tematykę nowych metod popełniania przestępstw na przykładzie rozwoju Internetu Rzeczy. Ma na celu ukazanie niebezpieczeństw związanych z brakiem odpowiednich zabezpieczeń przedmiotów będących częścią IR oraz usystematyzowanie aktualnego stanu wiedzy dotyczącego tej koncepcji. Autor na podstawie eksperymentów przeprowadzonych przez specjalistów od zabezpieczeń prezentuje sytuacje potencjalnie groźne dla każdego człowieka. Podjęto również próbę odpowiedniego zdefiniowania Internetu Rzeczy *stricte* na potrzeby krymialistyki.

Słowa kluczowe: Internet Rzeczy, cyberprzestępczość

Summary

The article deals with a subject of new methods of committing crimes with Internet of Things (IoT) as an illustration. Its aim is to present threats in a situations when there is a lack of decent securities in things which are part of Iot concept and to systematize state of knowledge about this conception. Based on recent experiments conducted by the security researchers, author depicts risks which could be very harmful. This article also sets forth to define IoT for the purposes of forensic and law studies.

Keywords: Internet of Things, cybercrime