KRYCY

Laboratorium nr 4

Wprowadzenie do OSINT i technik operacyjnych w kryminalistyce cyfrowej

Borkowski Mateusz
Gryka Paweł
Popiołek Paweł
Wawrzyńczak Michał

16 marca 2022

Spis treści

1 Wstęp

2 Zadanie do wykonania

Należało przeprowadzić reasearch w poszukiwaniu nowych technologi z potencjalną możliwością wykorzystania w działalności białowywiadowczej lub kryminalnej, oraz opisać kilka najciekawszych propozycji.

3 Znalezione technologie

- Szpiegowanie z wykorzystaniem dronów, z dużym zoomem
  - https://www.youtube.com/watch?v=gVP9a8$_b - NE$
- Drukowanie broni przy użyciu drukarek 3D
  - https://www.youtube.com/watch?v=C4dBuPJ9p7A
- Śledzenie przy użyciu rozwiązań typu AirTag
  - https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html
  - https://www.youtube.com/watch?v=EpiSzfMVPmg
- Odtwarzanie dźwięku z video
  - https://www.youtube.com/watch?v=eUzB0L0mSCI
- Przejmowanie kontroli za zdalnie sterowanymi pojazdami samochody/ciężarówki/traktory
  - https://physicsworld.com/a/how-to-hack-a-self-driving-car/
  - https://www.deere.com/en/news/all-news/autonomous-tractor-reveal/
- Wykorzystanie robotów w działaniach bojowych, np karabin na pise-robocie
  - https://www.theverge.com/2021/10/14/22726111/robot-dogs-with-guns-sword-international-ghost-robotics
- Wykorzystanie mikrofonów w słuchawkach TWS do podsłuchiwania
  - https://www.youtube.com/watch?v=Bq7xXlfEgJk
- Hackowanie słabo zabezpieczonego IoT wyposażonego w kamery i mikrofony
  - https://www.kickstarter.com/projects/domethics/turn-your-old-smartphone-into-a-gateway-for-home-automation?ref=discovery$_c ategory$
  - https://www.indiegogo.com/projects/audeze-filter/
- Możliwość analizy aktywności IoT do poznania czasowo-przestrzennych właścicieli
  - Wykorzystanie Wearables IoT, dla zwierząt, ludzi i dzieci.
  - https://www.cs.umd.edu/ nirupam/images/2$_p ublication/papers/LidarPhone_S enSys20_n irupam.pdf$
  - https://www.indiegogo.com/projects/flic-twist-the-wireless-dial-for-your-smart-home/
  - https://www.indiegogo.com/projects/revolo-smart-lock-the-ultimate-wifi-deadbolt/
  - https://www.kickstarter.com/projects/kiddowearable/kiddo-stay-connected-to-your-childs-wellbeing?ref=discovery$_c ategory$
- Włamywanie się do urządzeń typu *smart locks* w celu analizy-czasowo przstrzennej właścicieli mieszkania/domu, oraz włamywania się do miejsca ich zamieszkania

4 Hackowanie inteligentnych zamków

4.1 Czym są inteligentne zamki i na jakiej zasadzie działają

Inteligentne zamki są to urządzenia pozwalające na otwieranie różnego rodzaju drzwi bez konieczności użycia fizycznego klucza. Mogą być obsługiwane z użyciem mobilnej aplikacji bądź poprzez wpisanie ustalonego kodu na klawiaturze zamka. Coraz częściej najnowsze urządzenia tego typu integrują się z rozwiązaniami typu *smart home*, oraz łączą się z domową siecią WiFi. Wiele popularnych rozwiązań, w celu zwiększenia wygody, współpracuje z różnymi asystentami głosowymi typu *Google Assisant* czy *Amazon Alexa* (po wcześniejszym zintegrowaniu zamka z odpowiednim systemem) (1).

4.2 Popularność takich rozwiązań

Na różnego rodzaju serwisach aukcyjnych możemy zaobserwować rosnącą popularność tego typu rozwiązań. Do wyboru mamy rozwiązania różnych producentów, oraz działające w różny sposób. W tym paragrafie skupiamy się na analizie rozwiązań połączonych do sieci WiFi oraz zintegrowanych z systemami *smart home*. Przykładami takich rozwiązań są:

- Yale Assure Lock SL with Wi-FI and Bluetooth - shopyalehome.com
- Mechanizm Otwierania Drzwi Garażowych Meross Smart WLAN - amazon.pl

Powyżej mamy rozwiązania dwóch typów: inteligentny zamek mający zastąpić tradycyjny zamek do drzwi, oraz inteligentny mechanizm otwierania drzwi garażowych (oba z tych typów rozwiązań mogą być wykorzystane przez przestępców w podobny sposób, może również nastąpić jednoczesne ich wykorzystanie o czym w kolejnej sekcji).

4.3 Zagrożenia wynikające ze stosowania takich rozwiązań

Wraz z rozwojem branży *IoT* i systemów *smart home* należy spodziewać się coraz większej popularności rozwiązań *smart lock* (chociaż już są one bardzo popularne - można to zaobserwować np. po ilości opinii wystawianych pod produktami tego typu w różnych serwisach internetowych - 4.2). Zwiększona popularność doprowadzi do większej liczby producentów takich rozwiązań i pojawieniu się na rynku dużej ilości wątpliwej jakości produktów. Produkty takie mogą nie dostawać nowych poprawek bezpieczeństwa, bądź w ogóle być podatne na różne ataki od samego początku. Jednak ryzyko przełamania zabezpieczeń może dotyczyć wszystkich producentów. Warto zauważyć, że aby przejąc kontrole nad takimi urządzeniami, nie jest nawet konieczne przełamanie zabezpieczeń samego urządzenia. Przejęcie systemów z którymi takie urządzenie jest zintegrowane może okazać się wystarczające.

Jak wspomnieliśmy wcześniej, urządzenie zintegrowane ze *smart home* można kontrolować również za pomocą asystenta głosowego (można np. wprost zlecić otwarcie lub zamknięcie drzwi (2)). Tworzy to kolejne ciekawe wektory ataków, np. nieświadomy właściciel mógłby zostawić uchylone okno w pobliżu którego znajdowałby się głośnik z asystentem *Amazon Alexa*. W takim wypadku przestępca mógłby spróbować wywołać asystenta z zewnątrz i zlecić mu otwarcie drzwi.

W ogólności wykorzystywanie takich rozwiązań może prowadzić do dwóch rodzajów zagrożeń:

- złamanie zabezpieczeń takiego urządzenia w celu przełamania fizycznego zabezpieczenia domu/mieszka (np. w celu popełnienia przestępstwa kradzieży w włamaniem)
- przejęcie kontroli nad urządzeniem w celu prowadzenia analiz czasowo-przestrzennych skierowanych przeciwko właścicielom domów/mieszkań

W wypadku przejęcia całego systemu *smart home*, taka analiza w kontekście samych zamków może przybrać dość zaawansowaną formę. Kontrola nad zamkiem do drzwi oraz mechanizmem otwierania bramy garażowej może pozwalać na stwierdzenie nie tylko kiedy ktoś opuszcza dom lub do niego przychodzi. Przykładowo może dochodzić do prób stwierdzenia który z członków rodziny zamieszkujących dane gospodarstwo opuścił je i na jaki czas (np. każdy ma swój samochód za inną bramą garażową, a ktoś w ogóle z niego nie korzysta, albo jak ktoś do wyjścia nie zabiera ze sobą auta to prawdopodobnie wróci w przeciągu następnej godziny, w innych wypadku nie będzie go parę godzin).

Przeciwdziałanie

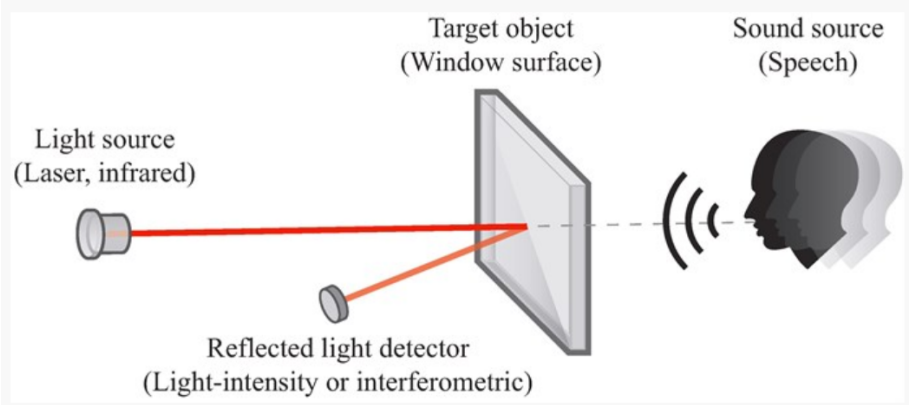
Naturalnym jest to że w scenariuszu w którym takie rozwiązania zyskują wielką popularność i są eksploitowane przez przestępców, pojawi się potrzeba przeciwdziałania takim technikom. Naszym zdaniem dobrym rozwiązaniem byłoby wprowadzenie regulacji prawnych którym podlegałyby takie

urządzenia. Takie regulację zobowiązywałyby producentów do wprowadzania regularnych poprawek bezpieczeństwa, oraz wyraźnego informowania konsumentów w jaki sposób korzystać z ich urządzeń aby poziom bezpieczeństwa pozostał na najwyższym możliwym poziomie. Nie wyeliminuje to problemu zupełnie, ale na pewno utrudni życie przestępcom.

5 Szpiegowanie za pomocą automatycznych odkurzaczy (3)

Coraz częstszym widokiem w domach średniozamożnych jest automatyczny odkurzacz wyręczający od przynajmniej części obowiązków związanych z sprzątaniem. Jednakże wraz z przyniesieniem do domu takiego sprzętu możemy zaprosić niechcianych gości. Urządzenia tego typu mają wiele funkcji, które potencjalni atakujący lub złodzieje mogliby wykorzystać:

- Mikrofon do nasłuchiwania na polecania głosowe - przy przyjęciu takiego sprzętu oczywiste jest ryzyko przesyłania nagranego przez odkurzacz dźwięku do atakującego. Rozwiązanie takie może być wykorzystywane bezpośrednio do podsłuchiwania mieszkańców, określenia godzin, w których mieszkańcy śpią, pracują i kiedy nie ma ich w domu (wtedy taki dom można na przykład okraść).
- Technologie laserowe LIDAR(Light Detection and Ranging) - technologia zaimplementowana w odkurzaczach w celu mapowania pomieszczeń. Oczywistym ryzykiem jest tutaj właśnie wyciek danych na temat rozmieszczenia obiektu w naszym domu, jednakże nie jest to ryzyko, na którym się skupimy. Ciekawszym ze względów technologicznych jak i bezpieczeństwa jest tu "podsłuchiwanie laserowe". Udowodniona, a nawet wykorzystana w prawdziwych atakach (6), została możliwość odczytywania drgań powierzchni wywołanych przez odgłosy za pomocą LASER'ów a następnie rekonstrukcji tych odgłosów za pomocą metod sztucznej inteligencji. Dlatego właśnie, gdy roboty wyposażone są w LIDAR'y, mają realną (7) możliwość podsłuchiwania ludzi w pomieszczeniu, w którym przebywają.



- Kamera - chyba nie trzeba tłumaczyć powstałego ryzyka.
- System operacyjny - w wielu autonomicznych odkurzaczach wgrane jest zwykłe (często przestarzałe) Ubuntu (5) z dużą liczbą nieużywanych funkcji i często łatwym do złamania hasłem (na przykład będącym nazwą urządzenia). Prowadzić to może do łatwego wektora ataku na domową sieć, najpierw przejęcia i zainfekowania komputera pokładowego robota, a następnie rozprzestrzenienia się na inne urządzenia w sieci.

Modelname	Model ID	Codename	Firmware	Soundfiles	SoC	RAM	Flash	MCU	WiFi	OS (Kernel)	Year
Xiaomi Vacuum Robot	rockrobo.vacuum.v1	ruby	ccrypt, unsigned	ccrypt, unsigned	Allwinner R16 (4x)	512 MByte	4GByte eMMC	STM32F103VCT6	RTL8189ETV	Ubuntu 14.04 (3.4.x)	Q3/2016
Roborock S5 / S50	roborock.vacuum.s5	rubys	ccrypt, unsigned	ccrypt, unsigned	Allwinner R16 (4x)	512 MByte	4GByte eMMC	STM32F103VCT6	RTL8189ETV	Ubuntu 14.04 (3.4.x)	Q4/2017
Roborock S6	roborock.vacuum.s6	tanos	A=enc(AES-256-CBC), signed (RSA)	A=enc, signed	Allwinner R16 (4x)	512 MByte	4GByte eMMC	STM32F103VCT6	RTL8189ETV	Ubuntu 14.04 (3.4.x)	Q2/2018
Roborock T6	roborock.vacuum.t6	tanos	A=enc(AES-256-CBC), signed (RSA)	A=enc, signed	Allwinner R16 (4x)	512 MByte	4GByte eMMC	STM32F103VCT6	RTL8189ETV	Ubuntu 14.04 (3.4.x)	Q2/2018

- Połączenie z chmurą - roboty te często wysyłają bardzo dużo informacji na serwery swojego producenta. Niektórzy użytkownicy pokazali, że potrafi być to nawet 11GB danych miesięcznie. Co ciekawe, w połączeniu z poprzednim punktem tworzy nam się nowe zagrożenie, na komputerach zawartych w tych urządzeniach znalezione między innymi narzędzie tcp-dump umożliwiające podsłuchiwanie ruchu sieciowego w przyłączonej sieci.

Przeciwdziałanie - czyli co robić i jak żyć

Przede wszystkim segmentacja sieci i odpowiednie ustawienie firewalla. Jeżeli urządzenie takie będzie znajdowało się w sieci dla gości, lub jeszcze lepiej, w sieci wyłącznie dla urządzeń IoT odciętej od internetu i sieci domowej, to znacząco zminimalizujemy możliwości ataków. Dodatkowo, zaczęły pojawiać się darmowe narzędzia za pomocą, których można usunąć niepożądane funkcje z naszych odkurzaczy (4). Niestety rozwiązania te wymagają trochę wiedzy i umiejętności, których niestety nie można oczekiwać od każdego użytkownika.

6 Przejmowanie kontroli nad zdalnie sterowanymi pojazdami

6.1 Wykorzystanie autonomicznych pojazdów

W ostatnim czasie zauważalny jest wzrost wszelkiego rodzaju pojazdów autonomicznych. Pojazdy sterowane przez sztuczną inteligencję wkraczają do coraz większej liczby obszarów gospodarki. Od kilku lat znane są już nie tylko koncepty, ale także realizację autonomicznych aut, które bez ingerencji człowieka potrafią poruszać się po drogach. W ostatnich latach zagadnienie to rozszerzyło się na inne typy pojazdów. W fazach działania są już m.in. roboty starship, czyli małe autonomiczne roboty, dostarczające jedzenie w kilku miastach świata. Na ostatnich targach CES zaprezentowane zostały autonomiczne ciągniki firmy JohnDeer. Sony pokazało autonomiczne/zdalnie sterowane i pokazali udane próby zdalnego sterowania z Tokio samochodem na torze we Frankfurcie. W odniesieniu do tak dynamicznego rozwoju, w wielu obszarach rodzi się wiele pytań odnośnie bezpieczeństwa i potencjalnych możliwości zagrożeń wynikających z nieuprawnionego dostępu do takiego pojazdu bądź całej grupy takich pojazdów.

6.2 Zagrożenia wynikające z wykorzystywania autonomicznych pojazdów

Autonomiczne pojazdy jak każda elektronika posiada swoje oprogramowanie, ich charakterystyka wymaga także, że muszą być podłączone do Internetu. Łączące te dwa fakty, istnieje prawdopodobieństwo zhackowania takiego urządzenia, i zakłócenia jego poprawnego działania.(10) Nie musi być to całkowite przejęcie kontroli nad takim pojazdem, w przypadku tak wrażliwych urządzeń często poruszających się wśród dużych skupiskach ludzi, wystarczy niewielka ingerencja aby taki pojazd stał się niebezpieczeństwem dla człowieka.
Poza oczywistymi przykładami gdy zaburzona zostaje praca autonomicznego pojazdu, co następnie doprowadza do wypadku, można wyobrazić sobie dużo ciekawsze i bardziej kreatywne zastosowania. Oto kilka przykładów, które udało nam się wygenerować podczas przeprowadzonej burzy mózgów. Przejmując kontrolę nad robotami dostarczającymi jedzenie jak np. wspomniany starship, możemy uzyskać podgląd i swego rodzaju mobilny monitoring, w momencie gdy mamy dostęp do całej floty takich robotów możemy obserwować dużą część miast. Dodatkowo z pozoru mało groźny "pojemnik na kółkach" w pojedynkę nie jest w stanie zbyt wiele zdziałać, natomiast cała wataha takich robotów działająca w skoordynowany sposób może np. skutecznie sparaliżować komunikację.
Myśl o zaprezentowany na niedawno odbywających się targach CES w Las Vegas, autonomicznym ciągniku firmy John Deer, także może budzić duży niepokój na myśl, że ktoś o złych zamiarach przejął nad nim kontrolę. W takim wypadku możliwe jest wiele tragicznych w skutkach scenariuszy. Ciągnik taki może dokonać ogromnych strat jeśli chodzi o plony rolne, a w konsekwencji prowadzić do braku żywności na danym obszarze. Poza tym kilkutonowa maszyna sterowana zdalnie, w momencie pojawienia się na drodze lub w dużym skupisku ludzi może stać się doskonałym narzędziem ataków terrorystycznych. Ta sam scenariusz dotyczy także wszelkiego rodzaju autonomicznych i zdalnie sterowanych aut, osobowych i ciężarowych. Nie musi być to nawet przejmowanie cudzych pojazdów, możliwość własnego zdalnie sterowanego pojazdu już daje ogrom możliwości wykorzystania w działalności przestępczej/terrorystycznej.
Warte wspomnienia są także wszelkiego rodzaju autonomiczne pojazdy i roboty wykorzystywane w gospodarstwach domowych są one często słabiej zabezpieczone niż pojazdy poruszające się w strefie publicznej. Mowa tu o odkurzacze, kosiarki i innych tego typu małych pojazdach. Dostanie się

do takiego urządzenia stwarza możliwości podglądania i podsłuchiwania przez kamery i mikrofony będące na pokładzie tych urządzeń.

6.3 Mitygowanie zagrożeń

Eksploitacja pojazdów autonomicznych typu samochody osobowe, ciężarowe, traktory, drony, pociągi z pewnością nie jest czymś co może wykonać, każdy. Natomiast, jak w przypadku każdej technologi istnieje możliwość przełamania zabezpieczeń, bądź wykorzystanie takiego pojazdu niezgodnie z jego pierwotnym przeznaczeniem.(8) Ważne jest zatem aby pojazdy te były należycie zabezpieczone.(9) Ciężko wskazać tutaj jakieś oczywiste sposoby zapobiegania takim sytuacją, poza wkładaniem dużych starań w zabezpieczenia tych systemów, częste poprawki bezpieczeństwa i ewentualne szybkie reakcje przy wydawanie poprawek w przypadku ujawnienia jakiejś podatności. Inną możliwością może być implementowanie w takich pojazdach osobnych systemów, odpowiedzialnych za reakcję w przypadku niestandardowych zachowań (np. wyłączenie urządzenia, odcięcie zasilania). Musiał by być to system całkowicie odrębny, nie powiązany w żadnym stopni z systemem głównym ani siecią, uniemożliwiło by to zdalne przejęcie takiego systemu, a ten mógłby reagować w sytuacjach niestandardowych/krytycznych.

7 Śledzenie przy użyciu rozwiązań typu AirTag

7.1 Co wyróżnia tego typu lokalizatory

Ostatnimi czasy, głównie ze względu na wypuszczanie na rynek takiego urządzenia przez Apple, dało się zauważyć znaczny wzrost popularności personalnych lokalizatorów. Głównymi przedstawicielami rozwiązań tej klasy są AirTag od Apple, SmartTag Samsunga oraz Tile. Zasada działania dla wszystkich jest bardzo zbliżona - urządzenia te emitują sygnał Bluetooth, który w momencie odebrania przez odpowiednie urządzenie (kolejno: IPhone/Android z aplikacją od Apple, Samsung Galaxy z włączoną opcją szukania lokalizatorów, smartphone z aplikacją Tile) zostaje rozszyfrowany i zinterpretowany. Następnie urządzenie odbierające sygnał wysyła do serwerów producenta informacje o obecnym miejscu położenia lokalizatora, która jest następnie przekazywana do właściciela lokalizatora. Warto zaznaczyć, że urządzenie, które znalazło lokalizator nie informuje o tym fakcie swojego właściciela (przynajmniej do czasu).

7.2 Jakie wynikają z tego zagrożenia?

Tak naprawdę w tym miejscu ograniczeniem jest tylko wyobraźnia. Dzięki spopularyzowaniu takich rozwiązań można nabyć takie urządzenie w każdym sklepie z elektroniką bez stwarzania jakichkolwiek podejrzeń oraz zostawianiu po sobie śladów, które mogłyby się pojawić w przypadku korzystania z profesjonalnych, stworzonych do śledzenia ludzi, urządzeń GPS, które mogą być na przykład dostępne tylko w sklepach dokładnie archiwizujących dane swoich klientów. Oznacza to, że za jedynie 150zł każdy jest w stanie śledzić dowolną osobę/pojazd na całym świecie bez większego ryzyka wykrycia. Potencjalnych scenariuszy wykorzystania takich urządzeń jest praktycznie nieskończenie wiele. Oczywistymi zastosowaniami jest śledzenie ludzi i pojazdów. Na przykład w celu uprowadzeń, poznania rozkładu dnia, kradzieży aut, włamywania się do pustych mieszkań. Nieoczywistym problemem tych rozwiązań jest, że można złośliwie wykorzystać również prywatny lokalizator ofiary. Sam jestem posiadaczem urządzenia SmartTag od Samsunga i zaskoczeniem było dla mnie, że za pomocą zwykłego smartphona i szukaniu urządzeń Bluetooth w okolicy można dowiedzieć się o obecności takiego urządzenia, pomimo faktu, że jest już ono "sparowane" z innym telefonem. W wypadku gdy ktoś nosi taki lokalizator przy kluczach do domu (prawdopodobnie jedno z najczęstszych zastosowań), można z zewnątrz domu, sprawdzić czy takie klucze (czyli i właściciel) znajdują się aktualnie w domu. Od razu nasuwa się pomysł utworzenia prostego urządzenia, na przykład na platformie Arduino wyposażonej w BLE, które umieszczone w pobliżu domu ofiary (w ogródku / na klatce schodowej) mogłoby z dużą dokładnością przez dłuższy okres czasu monitorować codzienną rutynę ofiary. Jest to na pewno dużo bezpieczniejsze i wygodniejsze rozwiązanie niż oddelegowanie ludzi do takiego zadania. Kolejnym, może bardziej abstrakcyjnym scenariuszem jest zastosowanie tych lokalizatorów do celów terrorystycznych, takich jak automatyczna, w wyznaczonym do tego miejscu na świecie, detonacja bomby umieszczonej w paczce. Poza konstrukcją bomby, cała reszta rozwiązania jest bardzo prosta i zautomatyzowana - co wyklucza błąd ludzki. Wyobraźmy sobie sytuację, w której ktoś masowo rozsyła takie paczki z celem detonacji w dowolnym szpitalu/stadionie/punkcie wyborczym. W wypadku ustalenia reguły na detonację w dowolnym punkcie wyborczym (na przykład wewnątrz przejeżdżającego obok pojazdu kurierskiego) można sparaliżować wybory w całym kraju, za pomocą czego można osiągnąć różne cele strategiczne. Jeśli ktoś słyszał o Theodorze Kaczynskim - Unabomberze (symbol terroryzmu w stanach przed 9/11) to takie scenariusze wcale nie wydają się niewykonalne. Śledzenie tras firm

kurierskich, w innym celu niż terroryzm, wykonał już jeden użytkownik platformy YouTube (11), który umieszczając AirTagi w paczkach transportowanych na różne miejsca na Ziemi był w stanie określić z jakich samolotów korzystają firmy kurierskie, gdzie składowane są paczki w trakcie swojej trasy oraz przez jakie kraje odbywa się tranzyt. Prawdopodobnie, przypadkowo udało mu się również wykryć nieczyste zagrania biznesowe firmy DHL, której w określonych okolicznościach, łatwiej było zgłosić zgubienie paczki i zwrócić pieniądze niż odsyłać ją do adresata.

7.3 Przeciwdziałanie

Firmy produkujące lokalizatory dodały funkcję (lecz dopiero po pewnym czasie) do urządzeń/aplikacji znajdujących, która powinna poinformować właściciela urządzenia, że od dłuższego czasu porusza się z nim ten sam, obcy lokalizator. W teorii to brzmi jak dobre rozwiązanie, jednak w praktyce informacja taka pojawia się zbyt późno (np. już po dotarciu ofiary do domu) lub wcale. W sprawie zabezpieczania swoich własnych lokalizatorów można rozważyć wkładanie ich do specjalnych pojemników zagłuszających jakikolwiek sygnał radiowy (takich jak do zapobiegania kradzieży aut z dostępem bezkluczykowym). Pytanie czy nie mija się to wtedy z celem istnienia takiego lokalizatora?

8 Podsumowanie

Z dnia na dzień na rynku pojawia się coraz więcej urządzeń mających za zadanie uczynić nasze życie wygodniejszym. Jak powszechnie wiadomo, (cyber) bezpieczeństwo i wygoda rzadko idą ze sobą w parze i wymagają kompromisów po obydwu stronach. Nie oznacza to jednak, że powinniśmy zamykać się na rozwój, ponieważ nic jest tak cyberbezpieczne jak stary dobry ciągnik Ursus lub "głupi" odkurzacz, który trzeba ciągnąć za sobą po mieszkaniu. Należy jednak świadomie podejmować decyzję o wdrażaniu "smart-rozwiązań" w swoje życie prywatne, tak aby rozumieć idące za nimi zagrożenia oraz mieć szansę przed niektórymi z nich się zabezpieczyć.

Literatura

[1] vivint.com - How Do Smart Locks Work?

[2] yalehome.com - Integrating with Amazon Alexa

[3] vaccum cleaners analysis

[4] build package for your vaccum cleaner

[5] information about many robot vaccum cleaners

[6] Eardropping in London's Ecuadorian embassy using LASERs

[7] Spying with Your Robot Vacuum Cleaner

[8] Connected and autonomous vehicles: A cyber-risk classification framework

[9] NIST cybersecurity risk management framework applied to modern vehicles

[10] How to hack a self-driving car

[11] Spying on delivery services