Bezpieczny inteligentny dom

(Secure smart house)

Piotr Szymajda

Praca inżynierska

Promotor: dr Paweł Rajba

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

7 lutego 2018

Streszczenie

W ostatnich latach obserwujemy ogromny wzrost liczby nowych rozwiązań opartych o Internet rzeczy, w tym również rozwiązań z obszaru tzw. inteligentnych domów. Niestety, równolegle z tym rozwojem pojawiają się nowe zagrożenia, a co za tym idzie nowe wyzwania związane z zabezpieczeniem tych rozwiązań. W tej pracy przedstawiam aktualnie dostępne rozwiązania stosowanych w inteligentnych domach wraz z ich zaletami oraz wadami, a także opisuje metodę analizowania zagrożeń i proces analizowania bezpieczeństwa systemów stosowanych w inteligentnych domach na kilku wybranych przykładach.

In recent years, we have seen a huge increase in the number of new solutions based on the Internet of Things, including solutions in the area of so-called smart homes. Unfortunately, along with this things new threats appear, and thus new challenges related to securing these solutions. In this paper I present currently available solutions used in smart homes with their advantages and disadvantages. Also I describe the method of analyzing threats and the process of analyzing the security of systems used in smart homes on several selected examples.

Spis treści

1 Wprowadzenie **7**

2 Co to znaczy „bezpieczny inteligentny dom”? **11**

2.1 Inteligencja urządzeń 11

2.2 Bezpieczeństwo domu 13

2.3 Zagrożenia 14

3 Podstawowe pojęcia **17**

3.1 Czym się różnią zagrożenie i podatność? 17

3.2 Autoryzacja kontra uwierzytelnienie, czyli co jest czym? 18

3.3 Różnica pomiędzy safety i security. 19

3.4 IoT, czyli czym jest Internet rzeczy? 19

4 Metoda analizy bezpieczeństwa **21**

4.1 STRIDE 22

4.1.1 Spoofing 22

4.1.2 Tampering 22

4.1.3 Repudiation 23

4.1.4 Information disclosure 23

4.1.5 Denial of service 24

4.1.6 Elevation of privilege 24

4.2 Zastosowanie STRIDE 25

5 Przegląd stosowanych rozwiązań 27

5.1 Zastosowane rozwiązania i technologie 28

5.1.1 Komponenty 28

5.1.2 Komunikacja wewnętrzna 28

5.1.3 Centralka 30

5.1.4 Rozwiązania komunikacji zewnętrznej 34

5.2 Modele do analizy 38

6 Analiza bezpieczeństwa wybranego modelu domu 39

6.1 Analizowany model 39

6.2 Odpowiedzialności poszczególnych elementów 40

6.3 Szczegółowe wyjaśnienie schematu działania instalacji 41

6.4 Analiza STRIDE 43

6.4.1 Wariant 1 - brak połączenia z Internetem 43

6.4.2 Wariant 2 - połączenie centrali do serwera 46

6.4.3 Wariant 3 - centrala w chmurze 49

7 Konkluzje 55

Bibliografia 57

Rozdział 1

Wprowadzenie

Od kilku lat możemy zaobserwować rosnące zainteresowanie tematem inteligentnych domów. Początkowo były konstruowane przez hobbystów i zapaleńców, dziś przez firmy specjalizujące się w projektowaniu systemów i urządzeń przewidzianych do instalacji w naszych mieszkaniach. Automatyzacja sterowania oświetleniem, ogrzewaniem czy multimediami zaczyna być standardem uwzględnianym przy budowie nowych domów czy przy remontach. W sumie trudno się temu dziwić. Wygoda, oszczędność, poczucie bezpieczeństwa, kolejna rzecz, którą można zaimponować znajomym. Zresztą automatyzacja już od dawna zaczęła wchodzić w prawie każdy aspekt naszego życia, pozwalając nam zaoszczędzić czas, zapomnieć o niektórych obowiązkach i skupić się na ważniejszych dla nas sprawach. Już od XIX wieku maszyny wyręczają nas w najróżniejszych domowych czynnościach. Począwszy od junkersów, pralek, lodówek, maszyn do szycia, przez zmywarki do naczyń i suszarki do ubrań, aż po tostery i czajniki elektryczne. Przez lata urządzenia te były udoskonalane i wyposażane w coraz to nowsze i wymyślne funkcje. Nic dziwnego, że w którymś momencie pojawiła się potrzeba, by sterować nimi zdalnie. Oczywiście najlepsze rozwiązanie powinno dawać nam możliwość połączenia się z tymi urządzeniami i wydawania im poleceń z dowolnego miejsca na świecie, by nie ograniczać nas do miejsca czy jakiegoś wymyślnego sposobu komunikacji. Tak więc przez wszelkiego rodzaju przełączniki, piloty, odbiorniki radiowe przechodzimy do najpopularniejszego dziś rozwiązania czyli Internetu. Sieć sieci, której historia sięga lat 60-tych, pozwalająca nam uzyskać dostęp do całego świata, zdaje się naturalnym wyborem w tej sytuacji. Tak oto, poczynając od tostera Johna Romkey'a z roku 1989, rozpoczyna się historia Internetu pełnego rzeczy pozwalających nam na dostęp do różnych informacji czy funkcji przez sieć. Trend ten dotyczy nie tylko typowego sprzętu gospodarstwa domowego, ale także wielu innych systemów znajdujących się w domach. Mam tu na my-

śli między innymi rozwiązania czuwające nad bezpieczeństwem mieszkańców, to znaczy wszelakie systemy wykrywania ruchu, czadu, pożaru, monitoringu wizyjnego czy zamków w drzwiach. Również te rzeczy uległy wielu modyfikacjom pozwalającym zintegrować je z ogólnie dostępną siecią i zarządzać nimi zdalnie.

Można by zatem pomyśleć, że czeka nas piękna przyszłość. Koniec z zostawionym zapalonym światłem czy włączonym żelazkiem. Koniec z zastanawianiem się, co się dzieje w domu, gdy jesteśmy poza nim i czy zamknęliśmy drzwi lub bramę. Koniec z zapomnianymi kluczami. Koniec niepotrzebnymi kosztami za prąd czy wodę. Domowy komputer (centralka) przypilnuje wszystkiego za nas. Będziemy mogli wyłączyć albo włączyć dowolne urządzenie zdalnie. Dostaniemy możliwość sprawdzenia, co się dzieje w domu w każdym momencie oraz pełnego monitoringu zużycia prądu czy wody w czasie rzeczywistym. Za pomocą naszego smartfona będziemy mogli sterować każdym aspektem naszego domostwa i to znajdując się w dowolnym miejscu na świecie, w którym będziemy mieli dostęp do Internetu. Nie dziwią zatem wyniki badań Berg Insight z roku 2015, według których na terenie Europy i Ameryki Południowej było już 17.9 milionów inteligentnych domów[1]. Sprzedaż inteligentnych urządzeń również bije wszelkie rekordy. Według danych IHS Markit w roku 2016 sprzedano i dostarczono 80 milionów urządzeń przeznaczonych dla inteligentnych domów, zwiększając tę liczbę o 64% w stosunku do poprzedniego roku[2]. Przy tak rosnącym trendzie podejrzewam, że za kilka-kilkanaście lat, niemalże każdy [1] będzie chciał mieć przynajmniej namiastkę inteligentnego domu. Czy to dobrze? Czy taka zmiana rozwiąże część naszych dzisiejszych problemów? Czy to rozwiązanie nie ma żadnych wad? „*Czy chcesz, żeby Twoja pralka była inteligentniejsza od Ciebie?*"[3]

Na powyższe pytanie przeczące odpowiedzi dają nam zarówno wizje pisarzy oraz reżyserów, jak i wydarzenia ze świata bezpieczeństwa cybernetycznego ze szczególnym uwzględnieniem Internetu rzeczy. W książce pod tytułem „Daemon" (Disc And Execution MONitor) autorstwa Daniela Suarez'a możemy przeczytać, jak inteligentny dom broni się przed próbami wdarcia do niego, pozostawiając ofiary wśród policjantów, agentów i antyterrorystów. W serialu zatytułowanym „Mr. Robot", możemy zobaczyć mniej krwawą scenę, w której grupa hakerów zmusza właścicielkę domu do przymusowej wyprowadzki, przejmując całkowitą kontrolę nad jej domem[4]. Można by odrzucić powyższe przykłady mówiąc, że to jedynie fikcja literacka. Niestety zarówno przywołana przeze mnie książka, jak i film zostały stworzone w oparciu o wiedzę specjalistów z zakresu cyberbezpieczeństwa i pokazują realne scenariusze. Ponadto

[1] Mam tu na myśli głównie osoby mieszkające w miastach lub w ich pobliżu

praktycznie codziennie dowiadujemy się o odkryciu nowych podatności[2] czy atakach na istniejące i funkcjonujące w naszych domach systemy. Oczywiście prawdziwe ataki na nasze mieszkanie nie muszą i prawdopodobnie nie skończą się tak jak w powyższych przykładach, ale czy na pewno chcemy zmienić swoje życie w „Big Brother'a" albo ciągłe próby ucieczki z domu sterowanego przez znudzonych nastolatków? Czy jesteśmy gotowi na wejście w świat, gdzie ktoś może zaszyfrować nam dane w lodówce i pokazać na jej wyświetlaczu prośbę o okup? Czy poradzimy sobie, gdy drzwi odmówią nam wejścia do naszego własnego mieszkania? Czy damy radę przetrwać, gdy to nie my będziemy sterować urządzeniami w naszym domu? Czy może da się stworzyć w pełni bezpieczny inteligentny dom? A jeśli nie, to jakie rozwiązania wybrać, by uczynić go jak najbezpieczniejszym?

[2]Słabość, która może zostać wykorzystana przez atakującego. W rozdziale 3.1 wyjaśniam czym różni się podatność od zagrożenia.

Rozdział 2

Co to znaczy „bezpieczny inteligentny dom”?

W tym rozdziale chciałbym rozważyć znaczenie słów „inteligentny” w kontekście domu oraz różnych urządzeń. Wytłumaczyć dlaczego, moim zdaniem, każdy dom powinien być tak zaprojektowany aby być bezpieczny. A także zastanowić się, jakie przykładowe zagrożenia czekają na budynki, zarówno te zwykłe, jak i inteligentne.

2.1 Inteligencja urządzeń

Zanim zacznę rozważać możliwe rozwiązania przy zabezpieczaniu inteligentnego domu, należy wyjaśnić, co rozumiem przez pojęcie „inteligentny”. Od kilku lat możemy zauważyć trend nadawania przymiotnika „inteligentny” rozmaitym urządzeniom codziennego użytku. Określenie to jest szczególnie wykorzystywane przez branżę reklamową, najczęściej w celu podkreślenia uniwersalności urządzenia, jego nietypowych funkcjonalności lub możliwości samoczynnego reagowania na różne zdarzenia. Codziennością stają się reklamy „inteligentnych” samochodów, pralek, telefonów czy zegarków. Od pewnego czasu daje się również zauważyć reklamy „smart” domów i mieszkań. Warto także pamiętać, że od dawna do grupy „inteligentnych” należy wiele fabryk oraz niektóre miasta. Co jednak kryje się za ich inteligencją? Czy faktycznie urządzenia te są zdolne do myślenia za swoich użytkowników? Czy może to tylko modne słowo wykorzystywane przez marketingowców?

Samo słowo „inteligentny” w stosunku do urządzeń pojawiło się przy bezpośrednim tłumaczeniu z języka angielskiego od słowa „smart”. Wyraz ten ma

jednak bardzo wiele znaczeń, częściowo znacznie odbiegających od naszego pojęcia inteligencji. Niektóre słowniki oraz poloniści krytykują używanie określenia inteligentny w odniesieniu do rzeczy[5]. Wyrażenie to jednak spopularyzowało się już na tyle, że dziś trudno byłoby nam zrezygnować z „inteligentnych” budynków czy zegarków.

Co zatem odróżnia „inteligentny” dom od zwykłego? Najprościej rzecz ujmując główną różnicą jest wyposażenie. Miano „inteligentnych” zyskały budynki wyposażone w różne czujniki do wykrywania m.in. ruchu, zmian temperatury, dymu oraz sterowniki służące do obsługi całej gamy urządzeń np. światła, rolet czy ogrzewania. W tym momencie napewno znalazłyby się osoby, które nie zgodziły by się ze mną, ponieważ wiele „zwykłych” domów również jest wyposażona w podobne systemy czy czujniki. Jest to jak najbardziej prawda. Rzeczą, która sprawia, że nasz dom zyskuje „inteligencję”, jest centralka, czyli mózg naszego domu. Jest to urządzenie, komputer, do którego spływają informacje ze wszystkich czujników. Dodatkowo, ten domowy komputer ma połączenie do wszystkich sterowników. Pozwala to na autonomiczne sterowanie domem na podstawie zaistniałych sytuacji. W zwykłych mieszkaniach, nawet tych wyposażonych w przeróżną automatykę, włącznik światła czy sterownik rolet obsługuje domownik. Natomiast w inteligentnych domach sterowanie to może odbywać się całkowicie bez udziału człowieka. Oczywiście centralka nie wymyśla sama, jaką decyzję ma w danej chwili podjąć. Jej zachowanie określa zbiór reguł zaprogramowanych przez twórcę całego systemu. Często sami mieszkańcy mają możliwość tworzenia i zmieniania istniejących zasad. W gotowych systemach, jest to dokonywane za pomocą prostych języków skryptowych takich jak Lua[6], lub za pomocą dedykowanych aplikacji[7]. W przypadku najprostszych rozwiązań wykonanych przez hobbystów, najczęściej trzeba przeprogramować program sterujący[8]. Co zatem stoi za inteligencją naszego domu? Oczywiście człowiek. Dom dopasuje się jedynie do sytuacji zaprogramowanych wcześniej przez programistę. Naturalnie, to również może ulec zmianie, gdy pieczę nad naszymi mieszkaniami przejmie sztuczna inteligencja zdolna do samodzielnego podejmowania decyzji oraz uczenia się na podstawie naszych reakcji czy upodobań[9][10]. Choć podejrzewam, że również one będą trafiały do nas z predefiniowaną czy konfigurowalną listą zasad.

Podsumowanie

Za inteligentny dom przyjmuję budynek mieszkalny posiadający komputer centralny, który na podstawie informacji pobieranych przez sieć czujników i zdefiniowanych scenariuszy jest w stanie sterować różnymi komponentami

mieszkania, bez potrzeby aktywnego udziału człowieka.

2.2 Bezpieczeństwo domu

Od zarania dziejów ludzie szukali schronienia. Począwszy od jaskiń, pierwszych szałasów czy ziemianek, poprzez różnego rodzaju domostwa z gliny, drewna czy kamienia, aż po dzisiejsze budynki. Dom miał zapewniać schronienie przed niesprzyjającymi warunkami pogodowymi, drapieżnikami oraz nieprzyjaciółmi, czy po prostu innymi ludźmi. Niezależnie od postaci, domy zakorzeniły się głęboko w historii człowieka oraz w praktycznie każdej kulturze, co możemy zauważyć w kształtach budowli czy przysłowiach. Dom jest, a przynajmniej powinien, być miejscem, w którym czujemy się komfortowo i bezpiecznie. Miejscem, w którym możemy bez obaw wypocząć czy cieszyć się swobodą i prywatnością. Często w domu znajduje się nasz majątek, który również chcielibyśmy chronić. Z tych powodów przez lata tworzone były najrozmaitsze rozwiązania mające za zadanie zagwarantować bezpieczeństwo nam i naszej własności. Poczynając od drzwi i zasuw, przez zamki, aż po skomplikowane systemy wykrywania intruzów. Bezpieczeństwo domów po dziś dzień jest kluczową składową braną pod uwagę przy projektowaniu i budowaniu praktycznie każdego budynku. Ochrona przed włamaniem, pożarem, zaczadzeniem czy zalaniem. Nowoczesne rozwiązania mogą ułatwić nam wykrywanie tego typu zagrożeń, abyśmy mogli w porę zareagować. Ponadto systemy te często zaprojektowane są tak, by samoczynnie reagować i choć częściowo przeciwdziałać tym zagrożeniom. Niestety wraz z nowymi rozwiązaniami pojawiają się nowe zagrożenia. Wzrost złożoności systemów ochronnych spowodował, że przestały one różnic się od zwykłych pecetów, a, co za tym idzie, są one równie podatne na ataki co nasze komputery. Często są one nawet gorzej zabezpieczone i skazane na brak aktualizacji od producenta, który porzucił wsparcie dla urządzenia. Tym samym, na inteligentne budynki czychają nowe, nieznane zwykłym domom, zagrożenia.

Podsumowanie

Przed architektami, projektantami, twórcami, nowych, inteligentnych, domów stoi zatem dodatkowe zadanie, by zabezpieczyć dom nie tylko od strony zagrożeń czysto fizycznych, ale również cybernetycznych. Jest to istotna kwestia, ponieważ, niezależnie od tego czy nasze mieszkanie jest inteligentne czy nie, najważniejsze, żebyśmy mogli czuć się w nim bezpiecznie.

2.3 Zagrożenia

Włamywacze, nawałnice, pożary, czad czy pęknięta rura wodociągowa to tylko niektóre z zagrożeń, które mogą przytrafić się każdemu domostwu. W związku z nimi instalujemy zamki w drzwiach, żaluzje w oknach, a wewnątrz czujniki dymu, czadu, ruchu, zalania. W inteligentnych domach systemy te często są zintegrowane z pozostałymi rozwiązaniami, pozwalając komputerowi centralnemu reagować na zdarzenia. Może on na przykład włączyć światła, alarm, uruchomić zraszacze, odciąć dopływ prądu czy wody, wezwać odpowiednie służby lub powiadomić nie przebywającego w domu właściciela. Można by zatem uznać, że komputeryzacja naszego domostwa rozwiązuje wiele problemów i dostarcza nam nowe możliwości chronienia domu oraz reagowania na różne zdarzenia. Niestety, jak już wspominałem w poprzedniej sekcji (2.2), wystawia ona nasz dom na nowe zagrożenia, które niesie ze sobą Internet. Sterowanie domem jest przydatne, póki znajduje się on tylko pod naszą kontrolą. Systemy nadzoru wizyjnego zapewniają nam bezpieczeństwo, dokąd tylko my możemy przez nie obserwować, co dzieje się w domu. Czujniki pozwalają reagować poprawnie na zdarzenia tak długo, jak działają bez przeszkód i nikt ich nie zagłusza lub nie podszywa się pod nie. Gdy zaczniemy się nad tym zastanawiać, powoli może okazać się, że każde podłączone do systemu inteligentnego domu urządzenie można obrócić przeciwko nam. Kosztem może być utrata prywatności, majątku czy nawet życia. Oczywiście na skomputeryzowane domy czeka więcej zagrożeń niż przejęcie nad nimi kontroli. Złośliwe oprogramowanie szyfrujące dane, wykorzystujące moc obliczeniową do „kopania” wirtualnej waluty czy korzystające z naszego łącza do atakowania innych celów to nic nadzwyczajnego w dzisiejszych dniach. Wiemy, jakie skutki może wywołać działanie tych programów na naszych komputerach, ale czy zdajemy sobie sprawę, jakie zagrożenia niosą one dla naszego domu? Mogą one spowolnić działanie naszego systemu, spowodować, że przestanie on odpowiadać lub poważnie go uszkodzić. Dlatego też zawsze należy poważnie zastanowić się, zanim podłączymy jakiekolwiek urządzenie do Internetu. Można by zatem zadać sobie pytanie, czy lepiej byłoby nie podłączać inteligentnego domu do Internetu i tym samym odseparować go od tych zagrożeń? Odpowiedź na to pytanie nie jest oczywista, ponieważ z jednej strony odcinamy dom od zagrożeń, ale również odbieramy mu możliwość komunikacji ze światem. Tym samym dom nie będzie w stanie wezwać służb czy powiadomić nas o jakimś zdarzeniu, gdy jesteśmy np. na wakacjach. Dodatkowo odbieramy możliwość automatycznych aktualizacji oraz pobierania wiadomości takich jak prognoza pogody czy różne ostrzeżenia, np. ze strony miasta o planowanym odcięciu prądu.

Podsumowanie

Jak widać na inteligentny dom czekają te same zagrożenia co na zwykły. Oczywiście dzięki rozwiązaniom technologicznym może on stawić czoła częsci z nich. Jednakże dodatkowo dochodzi kwestia ochrony systemów komputerowych sterujących domem. Jaką zatem architekturę rozwiązania wybrać, by była ona najbezpieczniejsza i jednocześnie nie ograniczała funkcjonalności domu? To postaram się w tej pracy omówić.

Rozdział 3

Podstawowe pojęcia

W niniejszym rozdziale chciałbym wyjaśnić znaczenie niektórych terminów, które pojawią się w tej pracy. Na szczególną uwagę zasługują te ściśle związane z bezpieczeństwem. Uważam je za bardzo istotne, ponieważ często są one ze sobą mylone, a ich złe zrozumienie może mieć bezpośrednie przełożenie na problemy z zabezpieczeniem systemu.

3.1 Czym się różnią zagrożenie i podatność?

Zagrożenie i podatność to dwa terminy nierozłącznie związanie z tematyką bezpieczeństwa i to nie tylko tą powiązaną z informatyką. Uznałem, że warto objaśnić ich znaczenia, ponieważ często są one mylone, a będę używał ich w tej pracy. Zatem zagrożenie jest to zjawisko lub zdarzenie, „*które powoduje, poczucie bezpieczeństwa maleje bądź zupełnie zanika.*"[11]. Innymi słowy jest to takie zdarzenie, które może być przyczyną różnych problemów lub katastrof (np. powódź). Przed zagrożeniami możemy się chronić, przewidywać, że wystąpią i minimalizować ich skutki. Inaczej natomiast jest z podatnością. Jest to pewna słabość danej rzeczy, która może zostać wykorzystana przez atakujących (np. dom leży na terenach zalewowych, albo zamek w drzwiach da się otworzyć każdym kluczem danego producenta). Jest to oczywiście pewne uproszczenie, ponieważ w kontekście informatyki słowo „podatność" ma wiele znaczeń w zależności od standardu[12]. Podatności najczęściej powstają w czasie procesu tworzenia danej rzeczy, np. poprzez błąd w oprogramowaniu stworzonym przez programistę, który nie przewidział jakiejś sytuacji, która hipotetycznie może się wydażyć. Niektóre z nich są bardzo trudne do wykrycia i potrafią przetrwać niezauważone przez wiele lat, jak na przykład głośne ostatnio podatności, Meltdown i Spectre [13], znajdujące się na prawie wszystkich procesorach

od 1995 roku[14].

Wspomniana na początku nierozłączność tych słów wynika z tego samego powodu co powiązanie słów „przyczyna" i „skutek". W pewnym uproszczeniu można przyjąć, że zagrożenie odpowiada przyczynie, a podatność jest słabością, która, w związku z zagrożeniem, może mieć negatywne skutki.

3.2 Autoryzacja kontra uwierzytelnienie, czyli co jest czym?

Kolejne dwa słowa, autoryzacja (*Authorization*) oraz uwierzytelnienie (*Authentication*), też są bezpośrednio związane z bezpieczeństwem, a dokładniej z procesem kontroli dostępu. W literaturze anglojęzycznej można też trafić na określenie „protokół AAA", którego nazwa jest skrótowcem od (Authentication, Authorization, Accounting)[15], czyli uwierzytelnienia, autoryzacji i księgowaniu[1]. Są to podstawowe składowe w praktycznie każdym systemie w którym mamy do czynienia z kontrolą dostępu. Przykładem jednego z takich systemów jest stosowany przy logowaniu do sieci protokół RADIUS[16].

Jak już wspomniałem uwierzytelnienie oraz autoryzacja są związane z procesem kontroli dostępu. Niepoprawne zrozumienie oraz implementacja, któregoś z nich, może umożliwić kompromitację rozwiązania. **Uwierzytelnienie** jest procesem weryfikującym kim jesteśmy, czyli na przykład poprzez sprawdzenie czy użytkownik o podanym loginie figuruje w systemie i czy dostarczone hasło jest poprawne. Innym przykładem jest podanie swojego imienia i nazwiska oraz hasła do kontaktu telefonicznego pracownikowi infolinii bankowej. **Autoryzacja**, z kolei, jest procesem weryfikującym czy jesteśmy uprawnieni, autoryzowani, do wykonania danej czynności, na przykład jest to sprawdzenie właściwości pliku pod kątem grup posiadających do niego dostęp, przed jego udostępnieniem lub potwierdzenie przez pracownika banku, że dzwoniąca osoba ma odpowiednie pełnomocnictwo do zarządzania danym kontem. Proces autoryzacji powinien nastąpić wyłącznie po pozytywnym przejściu procesu uwierzytelnienia[17]. W przeciwnym przypadku może dojść na przykład do takiej sytuacji: Do banku dzwoni osoba podająca się za menadżera tego banku i zleca wykonanie dużego przelewu. Menadżer jest osobą uprawnioną do wykonania takiej czynności, ale czy osoba która dzwoniła, na pewno nim jest?

[1]Księgowanie w sensie zapisywania, logowania, zdarzeń powiązanych z dostępem do sieci czy aplikacji

3.3 Różnica pomiędzy safety i security.

Kolejną parą problematycznych w zrozumieniu słów są angielskie „safety" oraz „security". Główny problem polega na tym, że oba oznaczają „bezpieczeństwo" mimo że w języku angielskim jest między nimi subtelna różnica. Zważywszy na to, że większość materiałów, z którymi miałem do czynienia, pisząc tę pracę, jest po angielsku, uznałem, że warto wytłumaczyć, czym różnią się od siebie te dwa wyrażenia.

Najprościej rzecz ujmując, system jest czyli bezpieczny(*safety*), jeśli nie generuje zagrożeń dla środowiska, w którym się znajduje. Na przykład weźmy system informatyczny służący do sterowania koleją. Możemy o nim powiedzieć, że jest bezpieczny(*safety*), jeśli wiemy, że nigdy nie doprowadzi on do sytuacji, że dwa pociągi znajdą sie na jednym torze, jadąc wprost na siebie. Z kolei jeśli o systemie mówimy, że jedną z jego cech jest to, że jest bezpieczny(***secure***), to mamy na myśli, że jest on odporny na zagrożenia zewnętrzne. To znaczy, że system będzie odporny na działanie atakujących, zapewnia spójność i integralność danych oraz ich poufność.

Warto również pamiętać o tym, że bezpieczeństwo(*safety*) musi być zarówno emocjonalne, jak i fizyczne[18]. Świetnym przykładem jest rodzicielstwo, ponieważ rodzice starają się zapewnić nie tylkom by dziecko czuło się dobrze, ale również starają się je chronić, by nie stała mu się żadna fizyczna krzywda. Przykładem sytuacji, w której nie zapewniamy pełnego bezpieczeństwa(*safety*), jest gdy dziecko leży w łóżku w swoim pokoju. Jest tam fizycznie bezpieczne(***secure***), ale jeśli boi się, że w szafie lub pod łóżkiem jest potwór, to i tak nie czuje się bezpiecznie(*safe*).

3.4 IoT, czyli czym jest Internet rzeczy?

Skrót **IoT** pochodzi z angielskiego *Internet of Things*, czyli Internetu rzeczy, przedmiotów [19]. Z uwagi na dość luźną ewolucję tego wyrażenia, nie ma ono jednoznacznej definicji. Jedną z nich określa, że jest to sieć połączonych urządzeń zdolnych do wymieniania między sobą informacji, przetwarzania ich lub gromadzenia za pomocą sieci Internetowej albo innej instalacji komunikacyjnej. Firma Gartner definiuje Internet rzeczy następująco: „*Jest to sieć fizycznych obiektów wyposażonych w technologię wbudowaną umożliwiającą komunikację, kontrolę oraz interakcję z własnym stanem lub otoczeniem zewnętrznym.*"[20]. O jakich obiektach mówi ta definicja? Na to pytanie świetnie odpowiadają historyczne początki IoT. Pierwszymi urządzeniami, które uzyskały

dostęp do Internetu, były automat z napojami (*1982*)[21], toster (*1989*)[22] i kamera transmitująca obraz ekspresu z kawą (*1991*)[23]. Co ciekawe, powstanie tego wyrażenia datuje się na rok 1999[24], czyli już po powstaniu wspomnianych wcześniej instalacji. Za jego twórcę uznaje się Kevina Ashtona, pracującego wówczas w MIT nad technologią RFID do zastosowania w firmie P&G. Jednak sam przyznał, że mimo iż pierwszy użył tego sformułowania, to i tak nie miał, i nie chciał mieć, wpływu na to, jakie znaczenie zyskało przez lata[24].

W mojej pracy mianem urządzeń IoT będę określał każdy komponent stanowiący element inteligentnego domu, który znajduje się w nim, ale z pominięciem centralki. Czyli, innymi słowy, będzie to każde urządzenie dostarczające danych do domowego systemu lub pozwalające na kontrolę przez ten system. Będą to na przykład przyciski na ścianach, termostaty, sterowniki żaluzji, światła czy czujki ruchu.

Rozdział 4

Metoda analizy bezpieczeństwa

Rozważanie bezpieczeństwa budynku niewątpliwie nie jest prostym zadaniem. Jak zatem zanalizować możliwe zagrożenia dla bezpieczeństwa różnych rozwiązań nie budując kilkunastu domów i nie zatrudniając grupy profesjonalnych włamywaczy czy hakerów, by przetestowali te rozwiązania? Odpowiedzią na to pytanie są modele analizy zagrożeń. Pomagają one znaleźć potencjalne zagrożenia dla naszego systemu, jeszcze na etapie jego projektowania. Dzięki temu możemy zaproponować mitygacje tych zagrożeń, czyli rozwiązania mające zniwelować ryzyko związane z ewentualnym wystąpieniem danego zagrożenia. Na przykład jeśli zagrożeniem dla naszego rozwiązania jest podsłuchanie występującej w nim komunikacji, to jako mitygację rozważamy szyfrowanie tych danych. Przy takiej analizie, zamiast budowy fizycznego domu czy implementacji aplikacji, stosujemy stworzony przez nas schemat reprezentujący rzeczy związane z bezpieczeństwem naszego systemu. Następnie stosujemy na tym schemacie wybrany przez nas model analizy zagrożeń w celu ułatwienia znajdywania zagrożeń oraz ich pewnego uporządkowania. Oczywiście, można by spróbować stworzyć własne modele, ale, moim zdaniem, lepiej zdać się na już przetestowane w boju rozwiązania, a jest ich trochę[25]. Metodyki te i im podobne stosuje bardzo wiele firm. Jedną z nich jest Microsoft, twórca modelu STRIDE [26], który to model zamierzam wykorzystać do analizy bezpieczeństwa inteligentnych domów i odpowiedzenia sobie na kluczowe pytanie w tym kontekście, czyli „Co może pójść nie tak?”. W tym rozdziale opisuję, czym jest model analizy zagrożeń STRIDE i z jakich części się składa oraz jakie ma on zastosowanie w przypadku inteligentnych domów.

4.1 STRIDE

Jak już wspomniałem we wstępie do tego rozdziału, twórcą modelu STRIDE jest firma Microsoft. Model ten został zaprojektowany, by pomóc przy analizie ryzyka architektury rozwiązania. Rozdziela on zagrożenia pod względem powodów i celów ataku. Jego nazwa pochodzi od pierwszych liter sześciu kategorii pod którymi będziemy rozważać poszczególne typy zagrożeń[27][28]. Są to:

1. **S**poofing – podszywanie się
2. **T**ampering – manipulacja (np. danymi)
3. **R**epudiation – zaprzeczalność (np. wykonania operacji)
4. **I**nformation disclosure – ujawnienie (wykradzenie) informacji
5. **D**enial of service – blokada dostępu do usług
6. **E**levation of privilege – podniesienie poziomu uprawnień

Należy pamiętać, że rozważane zagrożenia mogą należeć jednocześnie do kilku grup. Poniżej zamieszczam krótkie opisy każdej z kategorii.

4.1.1 Spoofing

Ze spoofingiem mamy do czynienia, gdy atakujący uzyskuje dostęp do systemu, korzystając z ukradzionej lub spreparowanej tożsamości. Mogą to być na przykład wykradzione innemu użytkownikowi uprawnienia. Warto pamiętać, że atakujący może podszywać się nie tylko pod użytkowników danego systemu, ale również pod poszczególne jego elementy. Szczególnie podatne są protokoły i rozwiązania, które nie zawierają mechanizmów potwierdzających prawdziwe źródło danej informacji. W ten sposób fałszowane są między innymi adresy mailowe wysyłającego lub numer dzwoniącego. Ma to na celu wprowadzenie odbiorce w błąd i uznanie, że kontaktuje się on z inną osobą. Po udanym spoofingu, kolejnym krokiem atakującego najczęściej jest eskalacja uprawnień (4.1.6) lub nadużywanie już posiadanych – np. zlecenie przelewu po podszyciu się pod menadżera banku.

4.1.2 Tampering

Tampering jest to nieautoryzowana modyfikacja lub wręcz sfałszowanie danych. Ten atak najczęściej ma miejsce, gdy dane przepływają z jednego

systemu do drugiego. Są one przechwytywane w trakcie i modyfikowane lub zastępowane innymi. Z tamperingiem mamy również do czynienia, gdy użytkownik ma możliwość przesyłania do naszego systemu danych, które są potem w jakiś sposób wykorzystywane w działającym systemie. Przykładem może być pole do logowania w które możemy wpisać dowolny ciąg znaków, a następnie zawartość tego pola, bez żadnych modyfikacji, zostanie wykorzystana w zapytaniu do bazy danych, czyli atak SQL injection.

4.1.3 Repudiation

Jest to zagrożenie wykorzystujący niemożliwość potwierdzenia wykonania jakiejś operacji przez danego użytkownika. Występuje on na przykład, gdy system nie loguje operacji wykonanych przez użytkowników, kiedy atakujący może łatwo zmodyfikować logi albo kiedy elementy systemu nie posiadają jednoznacznych identyfikatorów. Przykładem problemów z identyfikacją może być sytuacja, w której jedno z urządzeń ulegnie uszkodzeniu i zacznie rozsyłać wewnątrz sieci jakieś losowe komunikaty. W przypadku, gdy nie mamy wdrożonych procedur uwierzytelnienia[1], jedyna możliwość odnalezienia takiego urządzenia to odpinanie od sieci każdego po kolei i sprawdzanie czy źródło problemów zniknęło. Należy pamiętać, że atakujący również może zasymulować awarię jakiegoś sprzętu, np. by zmniejszyć czujność obrońców. Ataki z tej kategorii są bardzo problematyczne, ponieważ często bardzo trudno jest coś tutaj udowodnić. W takim przypadku, nawet profesjonalne firmy, zajmujące się analizą powłamaniową, potrzebują dużo czasu i wysiłku by do czegoś dojść. Ataki te najczęściej połączone są z innymi wymienionych tutaj kategoriami.

4.1.4 Information disclosure

Ujawnieniem informacji jest każde nieautoryzowane udostępnienie zastrzeżonych danych osobom, które nie mają do nich dostępu. Ataki te, często określane mianem wycieków danych, zyskują tym większy rozgłos, im więcej informacji zostało ujawnionych lub im bardziej były one wrażliwe. Do takich danych należą między innymi hasła, dane osobowe i kontaktowe. Innym przykładem są wycieki kodów źródłowych, dokumentów i treści korespondencji mailowej. Do tej kategorii należą również sytuacje, gdy atakujący uzyskuje dostęp do systemów monitoringu, czyli na przykład kamer, czujników ruchu, logów systemu. Pozyskane w ten sposób dane często są sprzedawane lub wykorzystywane do dalszych, skierowanych do konkrentych osób, ataków.

[1]Potwierdzenia tożsamości, dokładny opis w podrozdziale 3.2

4.1.5 Denial of service

Atak blokady dostępu do usług ma za zadanie utrudnić lub zablokować możliwość korzystania z systemu użytkownikom. Najczęściej jest to uzyskiwanie poprzez „zalanie" serwera pakietami, zlecenie mu trudnych obliczeń, wysłanie olbrzymiego pliku lub tak spreparowanych danych, by aplikacja, które je przetwarza, uległa awarii. Ataki te, nie tylko, mocno obciążają atakowane systemy, ale również są sporym wyzwaniem dla osób, które zarządzają tymi systemami. Podstawowym problemem jest odróżnienie połączeń od zwykłych użytkowników od tych serwowanych przez atakujących. Kłopot polega na tym, że obrońcy nie chcą dopuścić do sytuacji w której regularny użytkownik nie będzie miał dostępu do atakowanych usług, zatem nie można zablokować dostępu wszystkim, bo tego właśnie oczekuje atakujący. Dodatkowo część systemów przy dużym obciążeniu, w celu usprawnienia obsługiwania żądań, przestaje weryfikować dokładnie wszystkie dane, co może doprowadzić do wycieku lub nieautoryzowanej modyfikacji danych. Innym sposobem utrudnienia korzystania z usług może być zmiana języka systemu na koreański lub obrócenie interfejsu graficznego do góry nogami. Mimo że wydają się one mniej poważne, mogą bardzo utrudnić życie użytkownikom, co może doprowadzić na przykład do utraty popularności danego serwisu. Do tej kategorii zaliczają się także odcięcie zasilania oraz fizyczne uszkodzenie sprzętu, np. poprzez zalanie, zmianę temperatury czy wygenerowanie dużego hałasu[29].

4.1.6 Elevation of privilege

Z eskalacją uprawnień mamy do czynienia, gdy w systemie znajdują się użytkownicy z różnymi uprawnieniami do korzystania z pewnych funkcjonalności. Atakujący posiadający dostęp do konta z ograniczeniami poszerza swoje uprawnienia, uzyskując dostęp do uprzednio zablokowanych przed nim zasobów. Może to nastąpić na przykład poprzez zmianę flagi, w aplikacji lub bazie, oznaczającej uprawnienia do danej czynności. Innym przykładem jest wykorzystanie luki w systemie lub aplikacji, która umożliwi zmianę identyfikatora konta na przykłada na konto administratora. Jest to klasyczny etap ataku, w którym napastnik w pierwszej kolejności uzyskuje jakikolwiek, nawet najbardziej ograniczony, dostęp do systemu. Następnie poprzez eskalację uprawnień zdobywa dostęp do funkcji i danych zastrzeżonych, a na koniec wyprowadza zastrzeżone dane na zewnątrz.

4.2 Zastosowanie STRIDE do analizy zagrożeń dla inteligentnych domów

Modele takie jak STRIDE pomagają zrozumieć i odnaleźć problemy znajdujące się w naszym systemie czy aplikacji. Dzięki temu, jeszcze na etapie projektu, możemy wdrożyć odpowiednie rozwiązania w celu zabezpieczenia się przed danymi zagrożeniami. Jak już wspomniałem we wstępie do tego rozdziału, metody te używane są w wielu firmach. Jednak jest tu mały „haczyk". Polega on na fakcie, iż analizowane było głównie oprogramowanie, a w szczególności aplikacje webowe [30]. Tym samym trudno jest znaleźć jakieś odniesienia czy przykłady, które dałoby się zastosować w mojej pracy. Niemniej jednak, podział na kategorie, który został w niej zastosowany, znacząco zwiększa jej uniwersalność. Poza tym rozwiązania stosowane w inteligentnych domach, które będę poddawać analizie, tak bardzo nie odbiegają od tego jak, stworzone są zwykłe aplikacje.

Ponieważ celem pracy jest przetestowanie pewnej koncepcji analizy zagrożeń w kontekście inteligentnych domów, zastosuję rozwiązania jak najbardziej zbliżone do zwykłej architektury komputerowo-serwerowej. Znaczy to, że na przykład zamiast magistrali i protokołu Modbus[31] lub Zigbee[32], rozważę rozwiązania bazujące na modelu TCP/IP. Dokładniejsze wytłumaczenie, dlaczego decyduję się na pewne konkretnie technologie, opisuję w kolejnym rozdziale (5.1).

Rozdział 5

Przegląd rozwiązań stosowanych w inteligentnych domach

Zarówno w programowaniu, jak i w projektowaniu rozwiązań do zastosowania w inteligentnych domach te same problemy da się rozwiązać na wiele różnych sposobów, przy użyciu różnych technologii. Wybory, których dokonamy, mogą mieć bezpośredni wpływ na wiele aspektów, takich jak na przykład prędkość działania programu, złożoność, multiplatformowość czy bezpieczeństwo. Nie jest zatem niczym niezwykłym, że zazwyczaj decydujemy się na używanie rozwiązań i technologii, które znamy, dobrze rozumiemy i mamy doświadczenie przy posługiwaniu się nimi. Jeśli jednak nie możemy lub nie chcemy stosować starych metod, to nie wybieramy przypadkowej, tylko rozważamy kilka z nich. Bierzemy pod uwagę ich wady, zalety, cenę czy licencję, zanim zdecydujemy się na konkretny wybór. Nie inaczej jest w przypadku inteligentnych domów. Dodatkowo z oczywistych powodów nie jest możliwe rozpatrzenie wszystkich dostępnych możliwości ze względu między innymi na ich liczbę czy ubogą dokumentację niektórych rozwiązań. Z tego powodu w tym rozdziale opiszę pokrótce, niektóre technologie wraz z ich wadami i zaletami, a następnie uzasadnię, które z nich będę rozważał przy analizie zagrożeń i dlaczego. Dodatkowo, poniżej wyjaśniam, jakie założenia przyjmę, żeby uprościć model, w celu umożliwienia wykonania tego zadania.

5.1 Zastosowane rozwiązania i technologie

W budowanych dziś inteligentnych domach są stosowane bardzo różne rozwiązania, mimo to praktycznie w każdym z nich można wyróżnić następujące składowe:

1. urządzenia IoT stanowiące komponenty domu
2. rozwiązanie komunikacyjne pomiędzy komponentami i centralką
3. komputer centralny
4. rozwiązania sieciowe pozwalające na zdalne sterowanie i sprawdzanie informacji o domu

Oczywiście są one ze sobą ściśle połączone, tzn. wybór konkretnego modelu centralki definiuje nam, w jaki sposób możemy z nią komunikować urządzenia, czy w jaki sposób będziemy się do niej łączyć. Poniżej zamieściłem opisy wybranych technologii, z podziałem na wyżej wymienione składowe.

5.1.1 Komponenty

Zacznijmy od komponentów - mam tu na myśli wszystkie urządzenia, wchodzące w skład inteligentnego domu, znajdujące się w nim, poza centralką i urządzeniami sieciowymi. Możemy spośród nich wyróżnić czujniki, które jedynie dostarczają informację do systemu oraz te elementy, którymi możemy sterować. Sterowniki z kolei mogą być bardzo proste, na przykład zamykać i otwierać jakiś obwód tak jak to robi zwykły włącznik światła lub bardzo skomplikowane, posiadające wiele funkcji, jak na przykład pralka. Aby uprościć model nie będę rozważał konkretnych modeli żarówek czy piekarników. W tej pracy przyjmuję, że każde urządzenie, którym mogę w tym domu sterować, czy odbierać od niego informacje, jest po prostu prostym mikrokontrolerem. Zakładam też, że będzie ono posiadać identyfikator i zbór funkcji, które można na nim wywołać przesyłając do niego odpowiednie komendy.

5.1.2 Komunikacja wewnętrzna

Wszystkie te komponenty wewnątrz domu muszą się jakoś komunikować, odbierać i wysyłać komendy czy inne informacje. Jednymi z najczęstszych rozwiązań jest zastosowanie magistrali, zwykłych kabli sieciowych (RJ-45) lub

sieci bezprzewodowej. Każde z nich ma swoje wady i zalety. Zastosowanie **magistrali** ogranicza liczbę kabli, które dochodzą do centrali oraz pozwala łatwo dołączać dodatkowe urządzenia. Z drugiej jednak strony komunikaty rozsyłane magistralą dochodzą do wszystkich podpiętych urządzeń, a większość protokołów działających w takich rozwiązaniach nie obsługuje żadnej opcji szyfrowania. W momencie, gdy atakujący, przejmie jedno z urządzeń, bądź w inny sposób podepnie się do magistrali, będzie mógł podsłuchiwać całą komunikację. Do tego w danym momencie magistrali może używać tylko jedno urządzenie, co może wydłużyć czas reakcji niektórych komponentów. Stosowanie **sieci bezprzewodowej** minimalizuje liczbę kabli, ułatwia montaż instalacji w już istniejącym domu oraz jej rozwój i modyfikację. Dodatkowo możliwe jest by komponenty w przypadku utraty połączenia z centralą skomunikowały się pomiędzy sobą. Niestety część z tych zalet jest jedynie teoretyczna, ponieważ do urządzeń bezprzewodowych wciąż potrzeba dociągnąć kable zasilające, a problemy związane z samą technologią znacznie obniżają wygodę używania i stabilność działania systemu inteligentnego domu. Do tego, w sieciach bezprzewodowych, wciąż ograniczamy się do możliwości nadawania informacji tylko przez jedno urządzenie[1]. Poza tym, głównymi problemami w sieci bezprzewodowej są zakłócenia, niewystarczająca siła sygnału w niektórych partiach domu, oraz umożliwienie zdalnych ataków na Wi-Fi czy Bluetooth. Warto też pamiętać, że źródła zakłóceń w sieci bezprzewodowej, mogą być spowodowane różnymi czynnikami. Może to być włączona mikrofalówka[34], inne punkty dostępowe (np. u sąsiada), czy dedykowane urządzenia zakłócające[35] lub deautoryzujące[36][38]. Warto wspomnieć, że urządzenia takie wcale nie muszą być drogie, czy trudno dostępne.[2].

Wybór zwykłych **kabli sieciowych** chroni nas przed większością wyżej wspomnianych problemów. Dobre, ekranowane kable są praktycznie całkowicie odporne na zakłócenia pola elektromagnetycznego. Podłączenie każdego urządzenia osobno daje nam wiarygodność i stabilność systemu, a także możliwość komunikacji z wieloma urządzeniami praktycznie w tym samym czasie. Dodatkowo, jedyne możliwe ataki w takiej sieci są możliwe dopiero, gdy ktoś wejdzie nam do domu i zacznie je fizycznie wyciągać ze ściany. Zakładając oczywiście, że nie położymy kabli luzem po zewnętrznej ścianie budynku. Problemem, z którym borykają się sieci kablowe, jest między innymi ilość kabli, które musimy rozprowadzić po całym domu. Dodatkowo problematyczne może

[1]Gdyby kilka urządzeń próbowało jednocześnie nadawać informacje, w sieci bezprzewodowej, to doszło by do zjawiska interferencji, co zazwyczaj uniewożliwia odebranie wiadomości. W celu uniknięcia takich zdarzeń stosowany jest protokół CSMA/CA[33]

[2]Moduł esp8266 kosztuje ok 1-2 dolary[37], a gotowe rozwiązanie możemy znaleźć na Githubie[36]

być rozbudowywanie takiej sieci, ponieważ dołączenie nowych komponentów wymaga dociągnięcia nowych kabli.

Podsumowanie

Biorąc pod uwagę wady i zalety, na rozwiązanie bezprzewodowe można zdecydować się, gdy mamy już istniejący budynek i nie zamierzamy w nim robić dużego remontu lub mieć kabli poprowadzonych po wierzchu na ścianach. Przy takim wyborze powinniśmy poświęcić dużą uwagę sprawąom bezpieczeństwa komunikacji oraz źródłom ewentualnych zakłóceń. Osobiście jednak polecam użycie sieci opartych na kablach. Ze wspomnianych w poprzednim akapicie dwóch rozwiązań przewodowych, w tej pracy będę rozważał rozwiązanie bazujące na TCP/IP. Wybór ten jest podyktowany zarówno kwestiami bezpieczeństwa, jak i dużą bazą gotowych rozwiązań sieciowych, w tym szyfrowania i używania infrastruktury klucza publicznego[41]. Dodatkowym atutem jest duża dostępność informacji na temat tej technologii.

5.1.3 Centralka

Kolejnym i jednym z najważniejszych elementów jest centralka, serce, a w zasadzie mózg inteligentnego domu. Miejsce, do którego będą spływać wszystkie komendy i dane oraz będą tu podejmowane decyzje, zgodne z ustalonymi regułami, dotyczące wykonywanych akcji. Możemy tu zastosować szeroką gamę rozwiązań. Od prostych mikrokontrolerów, jak Arduino, przez tanie jedno-płytowe komputery[3], jak Raspberry PI, do zwykłych komputerów lub dedykowanych rozwiązań od producentów takich jak WAGO[39] czy Loxone[40]. Ponadto od kilku lat na rynku dostępne są rozwiązania chmurowe. Pozwalają one na podłączanie i sterowanie urządzeniami IoT z chmury. Każde z tych rozwiązań, ma swoje wady i zalety. Poniżej przedstawię kilka z nich oraz dokonam wyboru, które z rozwiązań zastosować w analizie zagrożeń.

Zaczynając od najprostszego i jednocześnie najtańszego[4] rozwiązania, czyli **programowalnych platform z mikrokontrolerem**. Pozwalają one na łatwe i szybkie zaprojektowanie prototypowych układów. Wyposażone w 8-bitowy mikrokontroler i ok. 32k bajtową pamięć, są w stanie pomieścić nawet trochę bardziej skomplikowane programy. Ich głównymi zaletami jest cena, pobór

[3] Z języka ang. single-board compute (SBC), komputery mieszczące się na pojedynczej płytce obwodu drukowanego, wraz z mikroprocesorem, pamięcią i portami wejścia/wyjścia[42]

[4] Chińskie Arduino UNO można kupić za ok 3$[43]

mocy, rozmiar oraz fakt, że wykonywany jest na nich jedynie nasz program. Dodatkowo możemy rozbudowywać układ za pomocą dedykowanych nakładek, np. „Ethernet shield" z portem RJ-45. Niestety do tych płytek bezpośrednio możemy podłączyć jedynie ograniczoną ilość urządzeń, a do tego każdą zmianę musimy samemu zaprogramować i wgrać na płytkę. Mimo rozrastającej się gamy gotowych rozwiązań, osobiście nie zdecydował bym się na sterowanie czymś więcej niż kilkoma urządzeniami w jednym pomieszczeniu za pomocą takiego urządzenia. Ponadto może być trudno zintegrować taką centralkę z rozwiązaniami umożliwiającymi zdalne sterowanie czy zmieścić na nich serwer udostępniający graficzny interfejs obsługi domu. Jednakże urządzenia te świetnie nadają się również do tworzenia własnych komponentów podłączanych do domowej sieci. Dzięki nim możemy łatwo stworzyć własny układ umożliwiający automatyzację urządzeń, takich jak np. toster. Poza tym, polecam używanie tych urządzeń przy hobbistycznych projektach, na przykład, kiedy chcemy stworzyć własny system sterowania światłami LED w swoim pokoju.

Kolejną propozycją, jest użycie **jedno-płytowych komputerów**, zwanych przez niektórych mikrokomputerami. Jest to trochę droższe rozwiązanie w porównaniu do poprzedniego[5], ale zapewniające nam większą moc i pamięć. Dodatkowo na tego typu urządzeniach mamy do dyspozycji system operacyjny. Pozwala to wgrać oprogramowanie do zarządzania domem czy komunikacji z gotowymi podzespołami lub nawet wymienić cały system na inny dedykowany do inteligentnych domów. Uniwersalność, niski pobór mocy, całkiem bogate wyposażenie[6], mały rozmiar, brak elementów chłodzenia[7] i niezbyt wysoki koszt powodują, że te mikrokomputery często wykorzystywane są do tworzenia domowych centrów multimedialnych czy kontrolowania wyświetlaczy monitorów w korytarzach lub na wystawach. Jeśli chodzi o ich zastosowanie w roli centrali inteligentnego domu, to niewątpliwie nadają się do tego znacznie lepiej niż takie proste układy jak Arduino. Ponadto w internecie można znaleźć sporo gotowych rozwiązań jak np. Domoticz[46] czy OpenHub[47], co znacznie upraszcza tworzenie inteligentnych systemów z ich użyciem.

Zastosowanie **zwykłego komputera** jako centralki sterującej domem jest dość popularnym rozwiązaniem w systemach budowanych przez hobbystów. Wybór ten nie różni się wprawdzie znacząco od zastosowania mikrokompute-

[5]Raspberry Pi 3 można kupić w Polsce za ok 170 zł[44]

[6]Bogate jak na tak małe urządzenie – np. Raspberry Pi 3 jest wyposażone w m.in. czterordzeniowy procesor, 1GB RAMu, 40 PINów GPIO, 4 wejścia USB, HDMI, Ethernet, WiFi, Bluetooth[45]

[7]Zaletą rozwiązań „fanless" jest to, że nie generują hałasu. Są one stosowane w urządzeniach, które praktycznie się nie grzeją, przez co nie wymagają chłodzenia.

rów, ponieważ w obu przypadkach mamy możliwość wgrania systemu operacyjnego lub dedykowanego oprogramowania. Wprawdzie przy tym rozwiązaniu mamy do dyspozycji większą moc obliczeniową i ilość pamięci operacyjnej, ale kosztem większego zużycia prądu, większego rozmiaru czy hałasu generowanego przez system chłodzący. Nie mają zatem istotnej przewagi nad mikrokomputerami, ponieważ systemy inteligentnych domów rzadko wymagają dużej mocy obliczeniowej.

Inną opcją jest zdecydowanie się na **dedykowane rozwiązania**. Pod względem funkcjonalności jest to prawdopodobnie jedna z najlepszych możliwości. Centralki te są zaprojektowane i wykorzystywane jedynie do celów sterowania i nadzorowania systemów inteligentnych budynków. Duże, wielo modułowe, instalacje mogą spokojnie obsługiwać całe wieżowce. Jedną z głównych zalet jest ich modularność, pozwalająca na rozbudowę systemu poprzez dołączanie do niego dedykowanych kontrolerów. Po instalacji, system konfiguruje się poprzez dostarczone przez producenta oprogramowanie, co znacznie ułatwia dostosowywanie go do potrzeb mieszkańców czy pracowników. Niestety rozwiązania te mają też kilka wad. Po pierwsze potrzebują trochę miejsca, by wszystko można było zamontować w uporządkowany sposób[48], nawet jeśli system nie ma jakiejś olbrzymiej ilości funkcji. Po drugie rozwiązania te często są dość drogie. Ostatnią wadą, dotykającą produkty niektórych producentów jest wymóg związania się z infrastrukturą sieciową producenta, w przypadku zewnętrznego sterowania domem, a co za tym idzie konieczność zaufania mu, że odpowiednio zabezpieczy on swoje systemy.

Jednym z najnowszych i dość ciekawych rozwiązań jest propozycja umieszczenia **centrali w chmurze**. Pojawienie się takiej opcji niewątpliwie podyktowane jest dynamicznym rozwojem tej technologii i odchodzeniem od budowania oraz utrzymania własnej infrastruktury. Najwięksi dostawcy usług chmurowych, czyli Amazon (AWS), Google (GCP) czy Microsoft(Azure), mają już w swojej ofercie wiele gotowych rozwiązań dla zarządzania systemami IoT. Niewątpliwą zaletą tego rozwiązania jest uproszczenie instalacji oraz łatwość zintegrowania go z innymi produktami chmurowymi. Ponadto pozwala to na jednoczesne zarządzanie wieloma urządzeniami, które mogą fizycznie znajdować się w różnych miejscach świata. Na takie rozwiązania decydują się między innymi duże firmy chcące zdalnie zarządzać wszystkimi budynkami, czy nawet flotą samochodową, wodną, czy lotniczą. Mimo oczywistego przeznaczenia tego typu rozwiązań bardziej do użytku „enterprise" niż prywatnego, uważam, że szybko pojawią się firmy[8], które będą oferować swoim klientom, właścicielom inteligentnych domów, systemy oparte właśnie na tych technologiach. Ponadto,

[8]Prawdopodobnie już istnieją lub są na etapie start-up'u

jeśli chcielibyśmy, na własną rękę, zbudować podobne rozwiązanie, to możemy spróbować to zrobić dość niewielkim kosztem[9]. Ogólny schemat wygląda następująco: urządzenia IoT, znajdujące się w domu, przesyłają informacje za pomocą tzw. „IoT Gateway'a"[10], do usług w chmurze, które agregują i przetwarzają je w zależności od konfiguracji. W zależności od źródła pochodzenia informacji lub innych czynników, takich jak czas czy stan pozostałych elementów chmury, informacje są przekazywane do odpowiednich serwerów, lambd[11] lub innych usług. Następnie w zależności od zaprogramowanych reguł są uruchamiana odpowiednie procedury, np. rozesłanie powiadomień, czy wysłanie odpowiedniej komendy z powrotem do jakiegoś urządzenia IoT. Głównymi zaletami rozwiązań chmurowych jest m.in. to że nie musimy martwić się o infrastrukturę i jej fizyczne bezpieczeństwo. Dzięki narzędziom pozwalającym na opisanie infrastruktury kodem, takim jak Terraform, Puppet czy stworzonym przez Amazona CloudFormation, możemy skonfigurować lub usunąć cały system w chmurze za pomocą jednej komendy[12]. Dodatkowo taka centralka będzie wysoko dostępna dla urządzeń zewnętrznych takich jak telefon użytkownika. Niestety w przypadku odcięcia połączania pomiędzy domem, a chmurą pozostawiamy urządzenia bez nadzoru centrali i bez możliwości sterowania nimi. Do tego dochodzi kwestia zaufania do dostawcy rozwiązań chmurowych. Pozostaje jeszcze problem kosztów, ale nie potrafię się do tego ustosunkować, ponieważ z jednej strony za wiele rzeczy w chmurze trzeba płacić i nawet, jeśli to niewielkie kwoty to potrafią szybko rosnąć, natomiast z drugiej strony, należy pamiętać, że nasze rozwiązanie nie jest nastawione na obsługę milionów użytkowników z całego świata, a co za tym idzie bardzo możliwe, że koszty korzystania z niego będą dość niskie.

[9]Koszt AWS IoT Core miesięcznie 0,0147$/urządzenie z data center w US albo 0,0176$/urządzenie z data center w Europie (np. Londyn, Frankfurt)[49], czyli za obsługę 1000 urządzeń zapłacimy ok 50 zł miesięcznie, 600 zł rocznie.

[10]Osobiście uważam, że to czysto marketingowa nazwa, ogólnie może to być zwykły router, ważne by mógł przetwarzać i przesyłać informacje, zapewnić szyfrowanie i pełnić funkcje firewall'a[52]

[11]Wprowadzona przez AWS w 2014 roku usługa umożliwiająca uruchamianie kodu w chmurze, która nie wymaga stawiania serwerów (*serverless*). Lambdy mogą zostać wywołane przez różne zdarzenia, np. pojawienie się nowego pliku w S3, o określonej godzinie lub w odpowiedzi na żadanie skierowane przez klienta do API[50]. W GCP podobna usługa nosi nazwę „Cloud Functions"[51].

[12]Dla Terraform'a są to odpowiednio komendy: *terraform apply* i *terraform destroy*

Podsumowanie

W tym podrozdziale, przedstawiłem najczęściej stosowane rozwiązania dla centralek inteligentnych domów wraz z ich wadami i zaletami. W analizie zagrożeń, przedstawionej dalszej części pracy, nie będę rozpatrywał ich wszystkich. W analizowanych modelach chciałbym użyć centralek zrobionych ze zwykłych komputerów lub minikomputerów.[13] Dodatkowo, chciałbym rozpatrzyć system oparty o usługi chmurowe, ponieważ jest to ciekawa technologia, której popularność wciąż rośnie oraz da mi to możliwość zadania sobie pytania „Czy przeniesienie centralki poza dom poprawi czy osłabi jego bezpieczeństwo?". Oba rozwiązania działają głównie za pomocą protokołu TCP/IP, więc część rozważań będzie spójna. Nie będę rozpatrywał użycia mikrokontrolerów, ze względu na ich prostotę oraz niską przydatność w roli centralek w takich systemach. Pod uwagę nie wezmę również rozwiązań dedykowanych, ze względu na zamknięty charakter części z nich oraz spore różnice pomiędzy niektórymi producentami.

5.1.4 Rozwiązania komunikacji zewnętrznej

W tym podrozdziale, chciałbym wspomnieć o możliwych rozwiązaniach pozwalających na zdalne sterowanie i nadzorowanie inteligentnego domu z zewnątrz. Oczywiście, praktycznie wszystkie opcje polegają na komunikacji z centralką za pośrednictwem Internetu. Wprawdzie wiele centralek systemów alarmowych, montowanych przez firmy ochroniarskie, łączy się za pomocą zwykłych modułów GSM z kartą SIM, ale nie będę rozważał tego rozwiązania z następujących powodów. Korzystając z sieci komórkowej mamy 3 opcje. Są to wykonanie/odbieranie połączenia głosowego, wysłanie/odebranie SMS'a, wysłanie/odebranie danych pakietowych. Ostatnia opcja sprowadza się do używania Internetu. Natomiast pierwsze dwie nie pozwolą na płynny przepływ informacji, w wystarczająco szybki sposób. Dodatkowo dojdzie nam opłata za utrzymanie tego numeru i za operacje, które będzie on wykonywał. Nie oznacza to, że centralka w ogóle nie powinna korzystać z usług GSM. W sytuacji awaryjnej, np. odcięcia Internetu lub wystąpienia jakiegoś ważnego wydarzenia, system inteligentnego domu powinien mieć możliwość skomunikowania się z właścicielem. Między innymi z tego powodu, warto rozważyć wyposażenie centralki w taki moduł. Osobiście, odradzałbym stosowanie połączeń GSM jako jedynej drogi komunikacji z inteligentnym domem.

[13] Nie będę ich rozróżniał, ponieważ rozwiązania te, z punktu widzenia bezpieczeństwa, nie różnią sie znacząco od siebie.

Komunikację zewnętrzną, za pomocą Internetu, możemy rozwiązać na kilka sposobów, z których część jest zależna od tego jaką centralkę wybraliśmy. Nie mam, w tym miejscu, na myśli jak będzie wyglądać aplikacja z której będziemy korzystać, czy jakich programów do połączenia możemy użyć. Dla centralki znajdującej się na terenie domu mamy kilka opcji. Po pierwsze możemy w ogóle **nie podłączać jej do Internetu**. Zabezpieczy ją to skutecznie przed zdalnymi atakami, ale również odbierze nam możliwość sterowania i nadzorowania domu, wysyłania powiadomień czy łatwego sprawdzania i ściągania aktualizacji[14]. Rozwiązanie to jest stosowane w budynkach o dużym znaczeniu strategicznym, jak laboratoria, elektrownie, zakłady produkcji wody itp. Jednakże, podłączenie do Internetu inteligentnego domu wydaje się mniej ryzykowne, a zarazem przynosi wiele zalet. Poza możliwością automatycznej aktualizacji i pobierania różnych przydatnych danych np. ostrzeżeń meteorologicznych, umożliwiamy opcję nadzorowania i zarządzania domem zdalnie z dowolnego miejsca na świecie. Będziemy mogli zdalnie zajrzeć czy wszystko jest w porządku oraz w razie potrzeby zareagować poprzez na przykład włączenie lub wyłączenie jakiegoś urządzenia, opuszczenie żaluzji czy otwarcie furtki. Przy wyborze odpowiedniej technologii, dom będzie w stanie wysyłać nam powiadomienia bezpośrednio na telefon, przekierować wideodomofon na nasze urządzenie czy wykryć, że do niego wracamy. Jeśli więc zdecydujemy się na podpięcie centrali do Internetu, to jedną z opcji jest **łączenie się bezpośrednio** do niej. Rozwiązanie to jednak wymaga, byśmy byli w tej samej sieci wraz z centralą, na przykład będąc wewnątrz domu. Należy jednak pamiętać, że stosując bezprzewodową łączność wewnątrz domu, nawet gdy nie jesteśmy podpięci do sieci, wciąż jesteśmy zagrożeni atakami z urządzeń, które znajdą się w pobliżu naszego mieszkania. Dodatkowo, rozwiązanie to nie jest zbyt dobre, ponieważ chcielibyśmy mieć możliwość sterowania domem także kiedy jesteśmy poza nim. Żeby usunąć, ten problem, potrzebny jest nam statyczny, publiczny adres IP. Wtedy będziemy mogli połączyć się do centralki z dowolnego miejsca na świecie, kierując nasze zapytania pod ustalony wcześniej adres. Problem w tym, że nie tylko my. Publiczny adres wystawia nas na ciągłe zautomatyzowane ataki, prowadzone przez boty, skanujące Internet w poszukiwaniu podatnych na znane ataki urządzeń. Do wad, zatem, trzeba doliczyć zwiększoną powierzchnię ataku. Musimy dodatkowo zabezpieczyć centralkę tak, by nikt poza nami nie miał do niej dostępu i nie był w stanie zmusić jej do wykonania jakiegoś polecenia lub zdradzenia jakiś informacji. W tym miejscu trzeba pamiętać, że zarówno proces uwierzytelnienia zachodzi bezpośrednio na naszej centrali. Z tego powodu musimy również zabezpieczyć się przed próbami ataków typu

[14] Jak pokazuje historia, jeśli chodzi o sprzęt IoT, to aktualizacje potrafią przysporzyć wiele problemów np. w telewizorach Samsunga[55] lub w „inteligentnych" zamkach do drzwi[56].

DoS, które spowodują że nasza centralka przestanie działać, a razem z nią cały inteligentny dom. Jak widać, rozwiązanie to wystawia nas na spore zagrożenie. Dodatkowo, w wielu przypadkach, niełatwo jest uzyskać stały, publiczny adres od operatora. Najczęściej nasze domowe łącze łączy nas z Internetem poprzez jeden lub więcej serwerów NAT[15]. W takim przypadku potrzebujemy połączyć się poprzez inny komputer, który posiada publiczne IP. Możemy się zdecydować, na gotowe rozwiązania lub skorzystać z własnego postawionego na **prywatnym serwerze**. Urządzenie to będzie pełnić rolę łącznika pomiędzy nami i naszą centralką. Może ono spełniać swoją rolę na dwa sposoby. Po pierwsze, możemy łączyć się przez ten VPS'a[16] do centrali, korzystając z jednego z trzech najpopularniejszych rozwiązań, do tunelowania połączenia, czyli stunnelu[17], reverse SSH[18] lub OpenVPN. Drugą opcją jest postawienie, na tym serwerze, programu, którego zadaniem będzie pośredniczenie w połączeniu do centrali. W odróżnieniu od poprzedniej opcji, gdzie komendy były przesyłane, od użytkownika do centralki, w niezmienionej formie, w tym wariancie, o tym co i kiedy zostanie przesłane do centrali, decyduje logika aplikacji znajdującej się na serwerze. Pozwala to wdrożyć dodatkową warstwę uwierzytelniania, umożliwia nam lepszy nadzór nad urządzeniami, chcącymi kontrolować dom oraz pozawala na zarządzanie wieloma centralkami. Mogą na tym skorzystać firmy dostarczające, tego typu rozwiązania, ponieważ używając tylko jednego publicznego adresu IP, mogą umożliwić wielu ludziom kontrolę nad ich domami, umożliwiając każdemu dostęp jedynie do jego systemu. Jeśli chodzi o kwestie bezpieczeństwa, to parę spraw się upraszcza. Domowa centrala, może filtrować przychodzące pakiety po adresie IP, co jest bardzo szybkie, a korzystając z któregoś ze wspomnianych rozwiązań, mamy zapewnione, bezpieczne, szyfrowane połączenie do serwera. Nie wystawiamy jej na bezpośrednie ataki, a jednocześnie nie odbieramy możliwości nawiązywania połączeń z Internetem. Dodatkowo, w przypadku udanego ataku typu DoS na serwer, centralka wciąż będzie trzymała pieczę nad naszym domem. Wadami tego rozwiązania jest potrzeba utrzymania serwera co łączy się z dodatkowymi kosztami[19] oraz potrzebą dobrego zabezpieczenia go i monitorowania jego stanu.

Ciekawym rozwiązaniem jest umieszczenie centrali poza domem, **w chmu-**

[15]Translacja Adresów Sieciowych (ang. *Network Address Translation*), inaczej maskarada IP - przesyłanie pakietów ze zmianą ich adresu docelowego lub źródłowego.

[16]Wirtualny Prywatny Serwer (ang. *Virtual Private Server*)

[17]Program autorstwa Michała Trojnara, pozwalający na tunelowanie połączeń TCP z użyciem TLSa[57]. Autora można spotkać na corocznej konferencji Security BSides Warsaw.

[18]„Odwrotny tunel"w SSH umożliwia przesyłanie połączeń przez serwer do klienta, poprzez bezpieczny kanał. Flaga do programu: -R[58].

[19]Koszty utrzymania własnego dość słabego VPSa, są bardzo niskie lub nawet, korzystając z oferty typu „Free Tier", darmowe [53][54].

rze, o czym wspomniałem w poprzednim podrozdziale (5.1.3). Komunikacja zachodzi tu zarówno pomiędzy centralką oraz „gateway'em" znajdującym się w domu, pozwalającym na połączenie się domowych komponentów z chmurą, jak i pomiędzy chmurą, a aplikacją na telefonie, za pomocą której chcemy sterować domem. Ze względu na zastosowane rozwiązanie, temat komunikacji zewnętrznej przeplata się z tematem działania samej centrali. Oczywiście, w chmurze możemy postawić zwykłe VPS'y i korzystać z nich podobnie, jak napisałem w poprzednim akapicie, ale szeroka gama rozwiązań oferowanych przez dostawców pozwala nawet na stworzenie struktury całkowicie pozbawionej serwerów[20], która będzie wstanie odpowiednio reagować i odpowiadać na wszystkie zdarzenia i komendy. Jest to ciekawe rozwiązanie z różnych względów. Przede wszystkim mamy przygotowaną, wysoko dostępną i w pełni skalowalną, infrastrukturę do sterowania urządzeniami IoT, o której bezpieczeństwo fizyczne czy rozwój nie musimy się martwić. Bezpieczeństwu teleinformatycznemu, również nie musimy poświęcać tak dużo uwagi jak w innych rozwiązaniach, ponieważ mamy do dyspozycji sprawdzone rozwiązania od dostawcy. Dobrze zdefiniowane i ustalone role oraz grupy bezpieczeństwa[21] pozwalają skutecznie odciąć większość dróg ataku na nasze rozwiązanie. Oczywiście nic nie jest bez wad. Głównym problemem, o którym już wspominałem, jest fakt, że odcięcie komunikacji domu ze światem zewnętrznym, pozostawia urządzenia IoT bez centrali. By temu zapobiec, powinniśmy zapewnić redundancję połączenia z siecią, na przykład poprzez umożliwienie „IoT gateway'owi" przesyłania danych przy pomocy telefonii komórkowej, w sytuacji awaryjnej. Dodatkowo problemem z którym spotkało się kilku programistów, jest sytuacja, gdy wyciekają nasze dane dostępowe do chmury. W tym momencie atakujący może całkowicie przejąć naszą infrastrukturę, co nie tylko narazi nas na utratę prywatności i przejęcie sterowania domem, ale również na wysokie koszty, jeśli na przykład na nasze konto zostaną zakupione maszyny kopiące kryptowaluty.

Podsumowanie

Powyżej, przedstawiłem przykładowe rozwiązania zapewniające i obsługujące komunikację zewnętrzną z inteligentnym domem. W analizie zagrożeń użyję rozwiązań z centralką całkowicie odciętą od sieci, połączoną poprzez

[20]Kod lambd wykonywany jest w kontenerach postawionych jedynie na czas wykonywania się lambdy i uruchamianych na wyznaczonej do tego przez dostawce infrastrukturze. Zatem z punktu widzenia klienta, nie posiada on na swoim koncie, żadnych serwerów.

[21]W AWS role to uprawnienia połączone z jakimiś danymi dostępowymi. Natomiast grupy bezpieczeństwa (*security groups*) to ustawienia firewalla. Konkretne nazwy, zależy od dostawcy rozwiązania, więc np. w GCP będzie się to nazywać inaczej.

VPSa oraz umieszczoną w chmurze, w celu przekonania się, czy podłączenie do sieci nie wystawia nas na zbyt wiele zagrożeń i czy zasadne są obawy o przeniesieniu centrali poza budynek, którym ma sterować.

5.2 Modele do analizy

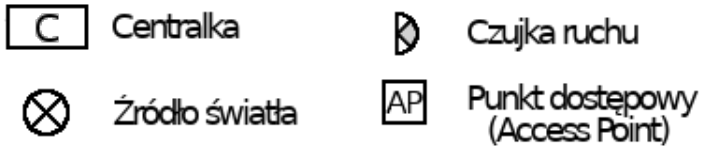
W tej pracy postaram się przeanalizować kilka modeli o różnej złożoności, każdy w trzech wariantach. Podział ten wynika z dwóch powodów. Pierwszy to trudność zanalizowania i opracowania dużego modelu. Z tego względu zacznę od bardzo prostych modeli „altanki", czyli jednopokojowego budynku z dwoma światłami i czujką ruchu. Następnie, dokładając kolejne komponenty oraz pomieszczenia, zamierzam przejść do całego domu. Drugi powód to chęć przeanalizowania różnych rozwiązań dla tych samych budynków. Pozwoli to zobaczyć, jakie wady oraz zalety mają poszczególne warianty i stwierdzić, które podejście najlepiej wybrać.

Warianty analizowanych modeli:

1. Centralka w domu - odcięta od sieci zewnętrznej
2. Centralka w dom oraz połączenie przez VPS
3. Centralka w chmurze

Wybór konkretnych technologii, które będą zastosowane w tych modelach, wraz z uzasadnieniem przedstawiłem wcześniej. Podsumowując, wszystkie rozważane modele będą składać się z nierozróżnialnych komponentów IoT, połączonych przy pomocy kabli sieciowych do centrali albo bramy sieciowej. Następnie wariant drugi, będzie komunikował się z naszym VPS'em, natomiast wariant trzeci z chmurą, z których to będzie wychodziła dalsza komunikacja, pozwalająca na sterowania i monitorowanie domu.

Do analizowanych modeli dołączone są poglądowe schematy. Na rysunku 5.1 przedstawiam tłumaczenie zastosowanych oznaczeń.



Rysunek 5.1: Legenda oznaczeń stosowanych w moich modelach

Rozdział 6

Analiza bezpieczeństwa wybranego modelu domu

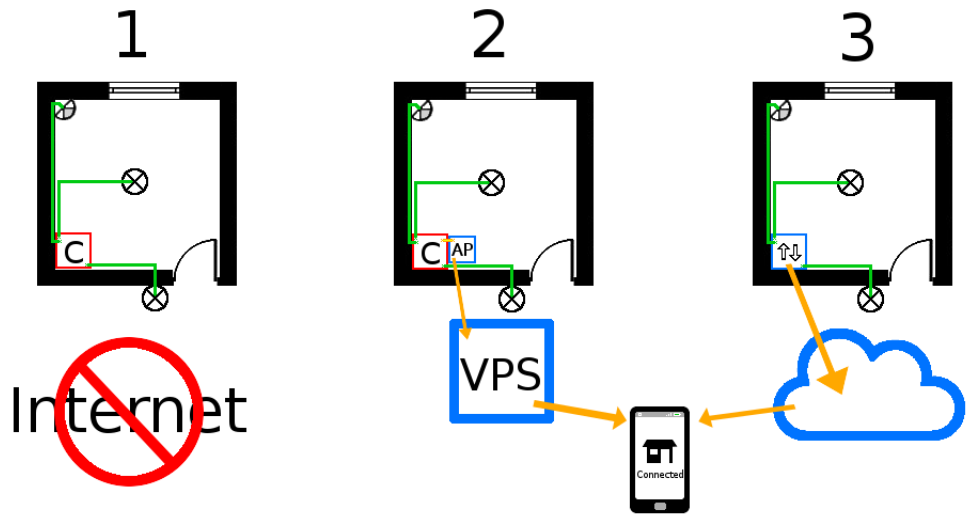
Kiedy weźmiemy plan przykładowego inteligentego domu to mnogość elementów występujących nawet w niewielkim mieszkaniu może zaskoczć. Jednakże, przyjęte przeze mnie w poprzednim rozdziale założenia pozwalają na sprowadzenie tego modelu do znacznie mniejszego, zawierającego jedynie kilka elementów, lecz porównywalnego pod kątem bezpieczeństwa. Poniżej przedstawiam ten model wraz z jego wariantami, o których wspomniałem w poprzednim rozdziale (5.2).

6.1 Analizowany model

Sprowadźmy nasz inteligentny dom do jedno pokojowego budyneku, na przykład altanka na działce lub w ogrodzie. Wyposażonego w:

- dwa źródła światła - jedno w środku i jedno przed drzwiami
- czujkę ruchu – wewnątrz
- przycisk bezstanowy – wewnątrz
- centralkę – wewnątrz w wariancie 1 i 2, w chmurze w wariancie 3
- łącze Internetowe – wariant 2 i 3

Model jest zrealizowany z użyciem wybranych w poprzednim rozdziale technologii, tzn. połączenia pomiędzy komponentami odbywają się po kablach sieciowych, centralka to zwykły komputer, wszystkie podłączone urządzenia IoT posiadają interfejs sieciowy. Poglądowe schematy przedstawiłem na rysunku 6.1.



Rysunek 6.1: Schematy trzech wariantów uproszczonego modelu. (1) odcięty od Internetu, (2) połączony do VPSa, (3) każde urządzenie wysyła dane do chmury poprzez „IoT gateway”

6.2 Odpowiedzialności poszczególnych elementów

- Centralka
  - zbieranie informacji z czujników (urządzeń IoT)
  - wysyłanie komend do urządzeń IoT
  - realizowanie zdefiniowanych scenariuszy[1]
  - odbieranie komend od użytkownika i ich realizacja
  - pobieranie dodatkowych informacji (pogoda, dostępne aktualizacje, zagrożenia, itp.)

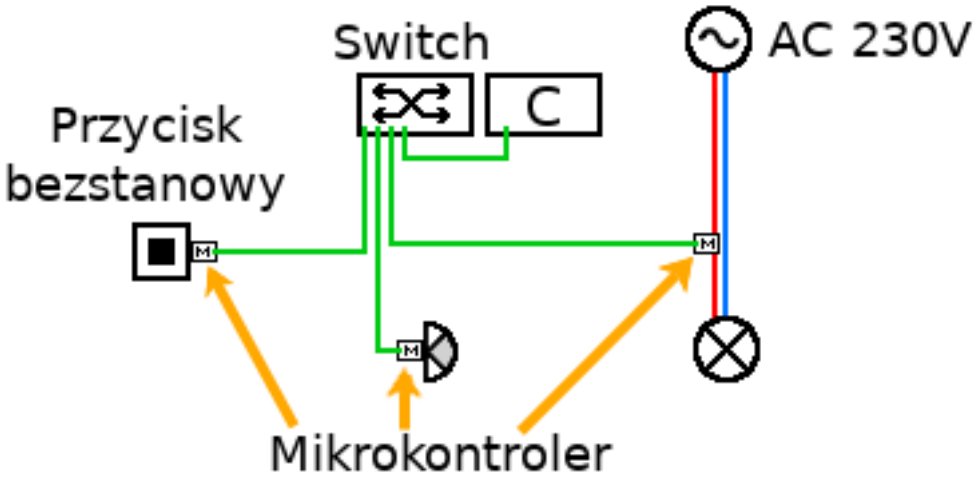
[1]Przykładowe scenariusze: **1)** Kiedy przycisk nr 2 zostanie wciśnięty jeden raz, to zapalają się światła nr 12 i 14, a kiedy ten sam przycisk zostanie wciśnięty trzykrotnie, w czasie 10 sekund, to wyłączy się światło w całym domu; **2)** O godzinie 7:00 odsłaniają się żaluzje w sypialni, a w kuchni uruchamia się ekspres z kawą.

- Punkt Dostępowy (*Access Point*)
  - udostępnianie dostępu do Internetu
- IoT Gateway
  - zapewnianie połączenia z usługami w chmurze
- VPS
  - wysyłanie/odbieranie informacji od użytkowników
  - wysyłanie/odbieranie informacji od centrali/centralek
- Centralka w chmurze
  - wysyłanie/odbieranie informacji od urządzeń IoT
  - realizowanie zdefiniowanych scenariuszy
  - wysyłanie/odbieranie informacji od użytkowników
  - pobieranie dodatkowych informacji (pogoda, zagrożenia, itp.)
  - integracja z innymi usługami w chmurze
- Program sterujący domem w formie aplikacji mobilnej lub przeglądarkowej
  - łączenie się do VPSa/chmury i pobieranie aktualnego stanu domu
  - umożliwienie wysyłania komend
- Urządzenia IoT
  - wysyłanie/odbieranie informacji od centralki

6.3 Szczegółowe wyjaśnienie schematu działania instalacji

Jak wspomniałem wcześniej, w tym modelu mamy tu do dyspozycji dwa źródła światła. Są one sterowane przez centralkę oraz dwa sensory: przycisk bezstanowy oraz czujkę ruchu. Zastosowanie przycisków bezstanowych w inteligentnych domach jest naturalnym następstwem zwielokrotnienia możliwości uruchomienia np. światła. W zwykłych domach, przełącznik światła przerywa

obwód zasilający. Jego stan definiuje, czy podpięte pod obwód urządzenia będą miały zasilanie czy też nie. Jednakże, w założeniach inteligentnego domu, jedno światło może zostać włączone przez różne czynniki, w zależności od zaprogramowanych reguł. Tak więc, na przykład może ono być uruchomione przy naciśnięciu przycisku, wykryciu ruchu, o konkretnej godzinie lub zdalnie. Tym samym, rola przełącznika sprowadza się do dostarczania do centrali informacji na temat czy został wciśnięty. Daje to możliwość zaprogramowania reguł tak, by ten sam przycisk wywoływał różne zdarzenia w domu w zależności od, na przykład, ilości naciśnięć w określonym czasie, dnia i godziny w której został użyty czy panującej pogody. Samo zjawisko wyłączenia światła wciąż polega na przerwaniu obwodu. Jest to wykonywane przez przekaźnik, sterowany za pomocą mikrokontrolera[59], który, w tym przypadku, za pomocą kabla sieciowego, jest połączony do centrali. Po odebraniu odpowiedniej komendy, mikrokontroler zmienia stan przekaźnika. Powyższy opis jest przedstawiony na rysunku 6.2. Urządzenia są na nim podpięte do centralki za pomocą przełącznika sieciowego (ang. *switch*). Jest to konsekwencja wyboru komputera jako centrali - ma on, zazwyczaj, tylko jeden port sieciowy. Chcąc zatem skomunikować wszystkie urządzenia ze sobą musimy użyć przełącznika.



Rysunek 6.2: Bardziej szczegółowy schemat układu sterowania światłem

Schemat ten pokazuje jak dokładanie działa system w inteligentnym domu oraz pozwala zauważyć podatne na atak punkty. Są nimi między innymi mikrokontrolery, kable czy centralka. Poniżej przedstawiam szczegółową analizę

zagrożeń trzech wspomnianych wcześniej wariantów, ułożoną zgodnie z modelem STRIDE.

6.4 Analiza STRIDE

Poniżej znajduje się analiza STRIDE przedstawionych wyżej wariantów, wraz z proponowanymi przeze mnie mitygacjami. Jak już wspomniałem w rozdziale 4.1, część zagrożeń lub mitygacji może powtarzać się pomiędzy grupami.

6.4.1 Wariant 1 - brak połączenia z Internetem

Spoofing

- Podszywanie się pod czujkę i ciągłe wywoływanie zdarzenia wykrycia ruchu - np. włącznie się światła.
- Podszywanie się pod żarówkę.
  - przejmowanie informacji skierowanych do niej - żarówka przestaje być responsywna.
  - mogą wystąpić problemy z naszą centralką, ponieważ są dwa urządzenia z tymi samymi identyfikatorami.
- Podszywanie się pod centralkę i wydawanie poleceń włączania/wyłączania światła.

Mitygacje

- Wprowadzenie certyfikatów i podpisów cyfrowych. Certyfikaty będą znajdować się na mikrokontrolerach oraz w centrali. W przesyłanym komunikacie można zaszyć aktualną datę i godzinę w celu uniemożliwienia atakującemu powtarzania podsłuchanych wcześniej pakietów.
- Wykrywanie, logowanie i powiadamianie o sytuacji wykrycia więcej niż jednego urządzenia z tym samym ID.

Tampering

- Wpięcie się w magistralę lub pojedynczy kabel centrala-urządzenie i modyfikacja lub tworzenie sygnałów.

- Wygenerowanie zakłóceń pola elektromagnetycznego w celu modyfikacji lub tworzenia sygnałów w kablach.

Mitygacje

- Stosowanie porządnych, ekranowanych, kabli, a jeśli to możliwe światłowodów.
- Poprowadzenie kabli w trudno dostępnych miejscach lub w ścianach.
- Wprowadzenie certyfikatów i podpisów cyfrowych. W przesyłanym komunikacie można zaszyć aktualną datę i godzinę w celu uniemożliwienia atakującemu powtarzania podsłuchanych wcześniej pakietów.
- Stosowanie kodów uwierzytelnienia wiadomości[2] - dołączanie do wiadomości jej skrótu, w celu zapewnienia jej integralności.
- Sprawdzanie poprawności przesłanych danych i ich ewentualna sanityzacja[3].

Repudiation

- Z powodu błędu w oprogramowaniu lub scenariuszu, może zdarzyć się coś nieoczekiwanego, np. wszystkie światła migają kilka razy zanim się wyłączą - chcemy mieć możliwość ustalenia czemu tak się dzieje, tzn. sprawdzenia który czujnik spowodował zaistnienie takiego zdarzenia, itp.
- Któryś z komponentów ulegnie awarii i chcemy ustalić który, bez odłączania wszystkich.

Mitygacje

- Zapisywanie historii wykonanych operacji i zaistniałych zdarzeń.
- Logowanie zdarzeń na centralce w katalogu o ograniczonym dostępie.
- Stosowanie procesu uwierzytelniania.

[2] Z angielskiego *message authentication code*, lub inaczej *message integrity code*
[3] Modyfikacja danych w celu zapewnienia ich poprawności[60]

Information disclosure

- Podsłuchiwanie informacji o wykrytym ruchu czy włączanym/wyłączanym świetle - z tych informacji potencjalnie wiadomo kiedy właściciel odwiedza dom, a kiedy go w nim nie ma.
- Wykradzenie logów z centralki.
- Wykradzenie informacji autoryzujących/certyfikatów z centralki.

Mitygacje

- Szyfrowanie przesyłanych wiadomości.
- Wprowadzenie certyfikatów i podpisów cyfrowych. W przesyłanym komunikacie można zaszyć aktualną datę i godzinę w celu uniemożliwienia atakującemu powtarzania podsłuchanych wcześniej pakietów.
- Zabezpieczanie dostępu do centralki i poufnych informacji takich jak logi, klucze prywatne, hasła itp.
- Stosowanie scenariuszy symulujących obecność mieszkańców w domu.

Denial of service

- Zalanie centrali komunikatami (po podszyciu się pod jedno z urządzeń IoT podpiętych do centrali).
- Odcięcie zasilania.

Mitygacje

- Filtrowanie pakietów/komunikatów.
- Stosowanie zasilania awaryjnego (*UPS*) oraz, jeśli bardzo zależy nam na ciągłym działaniu systemu, zastosowanie generatora prądu.

Elevation of privilege

- Po podszyciu się pod urządzenie wpięte do centrali, przekonanie jej by wykonywała nasze polecenia np:

- przesłała nam poufne dane (w tym logi)
- przyjmowała i rozdysponowywała w sieci nasze polecenia
- odebrała uprawnienia prawowitemu właścicielowi systemu

Mitygacje

- Kontrola dostępu, czyli stosowanie procesów uwierzytelniających i autoryzujących.
- Uniemożliwienie wysyłania poufnych plików poza centralkę.
- Szyfrowanie wrażliwych danych.
- Uruchamianie programów komunikacyjnych z niższymi uprawnieniami, bez dostępu do wrażliwych fragmentów systemu

6.4.2 Wariant 2 - połączenie centrali do serwera

W wariancie drugim występują wszystkie zagrożenia z wariantu 1, z uwagi na to, że jedyną różnicą jest podpięcie centralki do punku dostępowego, a co za tym idzie do Internetu. Dodatkowo odchodzą nam następujące zagrożenia:

Spoofing

- Podszywanie się pod serwer w połączeniu centralka-serwer lub serwer-użytkownik.
- Podszywanie się pod użytkownika (telefon, aplikację webową, itp.) przy połączeniu z serwerem.

Mitygacje

- Stosowanie rozwiązań takich jak VPN lub SSH - w celu zaszyfrowani komunikacji oraz skorzystania z gotowych narzędzi odpowiadających za proces uwierzytelniania.

Tampering

- Wysyłanie sfałszowanych wiadomości do/od serwera, użytkownika, centralki.
- Wysyłanie podsłuchanych wcześniej wiadomości, bez ich modyfikacji.

Mitygacje

- Stosowanie rozwiązań takich jak VPN lub SSH - w celu zaszyfrowani komunikacji oraz skorzystania z gotowych narzędzi odpowiadających za proces uwierzytelniania.
- Stosowanie rozwiązań zapewniających integralność przesyłanych komunikatów.

Repudiation

- Zmodyfikowanie lub usunięcie plików z logami na serwerze.
- Awaria lub błąd w aplikacji na serwerze - może spowodować wysyłanie do centrali losowych poleceń.

Mitygacje

- Tworzenie i przechowywanie w bezpieczny sposób logów na serwerze.
- Zapisywanie informacji przesłanych przez serwer w logach w centralce.

Information disclosure

- Podsłuchiwanie komunikacji przychodzącej i wychodzącej z serwera.
- Podsłuchiwanie komunikacji do centrali.
- Wykradzenie informacji/logów/certyfikatów.
- Po uzyskaniu nieautoryzowanego dostępu można „podglądać” co się dzieje w domu.

Mitygacje

- Stosowanie rozwiązań takich jak VPN lub SSH - w celu zaszyfrowani komunikacji oraz skorzystania z gotowych narzędzi odpowiadających za proces uwierzytelniania.
- Szyfrowanie wrażliwych danych.
- Wykrywanie ilości podłączonych użytkowników oraz zapisywanie w logach miejsc z których się łączą się użytkownicy w celu późniejszej analizy.
- Filtrowanie i blokowanie pakietów za pomocą zapory - np. *iptables*.

Denial of service

- Zalanie serwera pakietami.
- Zagłuszanie Internetu w pobliżu klienta łączącego się do serwera.
- Blokowanie przesyłanych pakietów od klienta do serwera lub od serwera do centrali.
- Odcięcie domu od Internetu.
- Odcięcie zasilania lub Internetu od centrum obliczeniowego w którym znajduje się nasz serwer.

Mitygacje

- Filtrowanie i blokownie pakietów przy pomocy zapory - np. *iptables*. Można to prosto uzyskać, ponieważ serwer ma stały adres, więc centralka nie powinna przyjmować pakietów innych niż od niego.
- Odpowiednia konfiguracja programów stosowanych do komunikacji (np. sshd na serwerze) i zablokowanie nie używanych przez nas możliwości połączenia z serwerem.
- Wybranie dużego dostawcy rozwiązań serwerowych - lepsze zabezpieczenia fizyczne, wyższy poziom świadczenia usług[62].
- Jeśli ktoś po drodze blokuje nasz ruch, można użyć VPNa.
- Redundancja połączenie z serwerem np. dwa kable od różnych dostawców oraz moduł GSM z kartą SIM i Internet bezprzewodowy (mobilny).

- Utworzenie rozproszonej sieci serwerów, rozłożonych w różnych strefach dostępności, z użyciem grup autoskalujących w celu automatycznego postawienia nowej instancji gdy poprzednia ulegnie uszkodzeniu.

Elevation of privilege

- Atakujący uzyskuje dostęp do konta z minimalnymi uprawnieniami, a następnie, wykorzystując jakieś podatności w oprogramowaniu na naszym serwerze, poszerzyć te uprawnienia. Po uzyskaniu uprawnień administratora atakujący może praktycznie wszystko, tzn. kontrolować cały dom, wykraść dane znajdujące się na serwerze itp.

Mitygacje

- Nie uruchamianie aplikacji z uprawnieniami administratora jeśli to nie jest konieczne.
- Konteneryzacja aplikacji jeśli jednak potrzebuje ona dostępu na poziomie administratora.
- Monitorowanie i informowanie o uzyskaniu dostępu do konta administratora.

6.4.3 Wariant 3 - centrala w chmurze

Wariant trzeci podobny do wersji drugiej, ale tym razem w domu nie ma urządzenia centralnego. Wszystkie czujniki i sterowniki są połączone z chmurą, gdzie przesyłają i skąd odbierają wszystkie informacje[61]. Dostawcy chmurowi udostępniają różne usługi, które umożliwiają łatwe wdrożenie takiego rozwiązania. Z tego powodu, nie wszystkie wymienione wcześniej zagrożenia występują w tym wariancie, dlatego część wpisów będzie powtarzać sie w stosunku do poprzednich list.

Spoofing

- Podszywanie się pod chmurę - wysyłanie do urządzeń komunikatów, które udają te z wysłane z centrali w chmurze.
- Podszywanie się pod komponent podpięty do chmury - podłączenie się do centrali jako jedno z urządzeń IoT.

- Podszycie się pod użytkownika/administratora i uzyskanie dostępu do panelu sterowania chmurą lub do interfejsu programistycznego.

Mitygacje

- Używanie kluczy, certyfikatów i szyfrowanych tuneli.
- Ograniczenie uprawnień użytkownikom chmury.
- Monitorowanie dostępu do konta administratora w chmurze.
- Tworzenie i korzystanie z kont o ograniczonej funkcjonalności.

Tampering

- Przechwytywanie, fałszowanie, zmienianie wiadomości na połączeniu chmura-komponent oraz chmura-użytkownik (telefon, aplikacja przeglądarkowa, itp.)
- Wygenerowanie zakłóceń pola elektromagnetycznego w celu modyfikacji lub tworzenia sygnałów w kablach prowadzących do urządzeń IoT.

Mitygacje

- Stosowanie porządnych, ekranowanych, kabli, a jeśli to możliwe światłowodów.
- Szyfrowanie i podpisywanie danych.
- Sprawdzanie poprawności przesłanych danych.
- Stosowanie kodów uwierzytelnienia wiadomości - dołączanie do wiadomości jej skrótu, w celu zapewnienia jej integralności.

Repudiation

- Zmodyfikowanie lub usunięcie plików z logami tworzonymi w chmurze.
- Awaria któregoś z urządzeń podpiętych do centrali w chmurze - z uwagi na dużą ilość podłączonych urządzeń IoT oraz odległość pomiędzy nimi, a centralą, chcielibyśmy umieć łatwo określić, które z nich uległy awarii.

Mitygacje

- Zapisywanie w logach informacji dotyczących zaistniałych zdarzeń.
- Przechowywanie logów w bezpiecznym miejscu, w chmurze np. na zabezpieczonym, prywatnym S3 (*AWS*).
- Stosowanie procesów uwierzytelniania w celu identyfikacji i potwierdzenia pochodzenia komunikatu z konkretnego urządzenia IoT.

Information disclosure

- Po przejęciu dostępu do chmury atakujący ma pełen dostęp do podglądania i sterowania domem, a także możliwość przekonfigurowania infrastruktury oraz zakupu wielu drogich maszyn w celu kopania kryptowalut.
- Po podszyciu się pod użytkowania atakujący ma dostęp do wszystkich informacji, do których dany użytkownik ma dostęp.
- Pobranie z naszych usług plików do których dostęp nie został zablokowany.

Mitygacje

- Szyfrowanie wrażliwych informacji.
- Monitorowanie dostępu do chmury, w szczególności do funkcji administratora.
- Nie używanie haseł, blokowanie nieużywanych portów, włącznie dwu etapowej weryfikacji tam gdzie to możliwe.
- Upewnianie się, że dane dostępowe do AWS nie są przechowywane tam gdzie ich nie trzeba i nie powinno być - w szczególności nie są zapisane nigdzie w kodzie albo w zmiennych systemowych.
- Sprawdzenie uprawnień i konfiguracji naszych zasobów pod kontem dostępności - np. pliki znajdujące się na dysku S3 mogą być publicznie dostępne, zatem nie jest dobrym pomysłem żeby były to akurat nasze logi lub inne pliki zawierające wrażliwe informacje.

Denial of service

- Uniemożliwienie połączenia komponenty - chmura (np. przecięcie kabla Internetowego).
- Wysłanie do chmury olbrzymiej ilości fałszywych pakietów - w zależności od dostawcy i konfiguracji, może to znacznie zwiększyć rachunek albo spowodować znaczne opóźnienia w realizacj żądań od komponentów.

Mitygacje

- Filtrowanie pakietów względem źródła.
- Redundancja połączenie z serwerem np. dwa kable od różnych dostawców oraz moduł GSM z kartą SIM i Internet bezprzewodowy (mobilny).
- Utworzenie rozproszonej sieci serwerów, rozłożonych w różnych strefach dostępności, z użyciem grup autoskalujących w celu automatycznego postawienia nowej instancji gdy poprzednia ulegnie uszkodzeniu.
- Korzystanie z rozwiązań „bezserwerowych" - uruchamiających odpowiedni kod jedynie w ustalonym momencie, za każdym razem na nowo - np. Lambdy (*AWS*).

Elevation of privilege

- Uzyskanie dostępu do konta użytkownika lub podszycie się pod urządzenie IoT, a następnie wykorzystanie tego do uzyskania dostępu do funkcji administratora i przejęcie całej infrastruktury.
- Po podszyciu się pod urządzenie komunikujące się z naszą chmurą, wykorzystanie zbyt szerokich uprawnień w dostępie do zasobów w chmurze.

Mitygacje

- Tworzenie osobnych roli dla każdej grupy z maksymalnie ograniczonymi uprawnieniami, ponieważ na przykład termometr znajdujący się w naszym domu, nie powinien mieć uprawnień do tworzenia i usuwania instanicji serwerów czy pobierania logów.
- Nie uruchamianie aplikacji z uprawnieniami administratora jeśli to nie jest konieczne.

- Konteneryzacja aplikacji jeśli jednak potrzebuje ona dostępu na poziomie administratora.
- Monitorowanie i informowanie o uzyskaniu dostępu do konta administratora.

Rozdział 7

Konkluzje

Analiza zagrożeń, z użyciem modelu STRIDE, wyraźnie pokazuje, że, niezależnie od wybranego rozwiązania, musimy zwrócić wyraźną uwagę na jego poprawne zabezpieczenie. Zatem, gdy nie zależy nam na zdalnej kontroli, wystarczy, że nasz inteligentny dom zabezpieczymy przed atakami wymagającymi fizycznego podłączenia się do naszej infrastruktury, więc także włamania się do naszego domu. Mimo ograniczonych możliwości tego rozwiązania, w porównaniu do innych, wciąż może ono pomóc w zautomatyzowaniu wielu, wykonywanych przez nas na co dzień, czynności. Kiedy zależy nam na możliwości zdalnego nadzorowania i sterowania domem, możemy wykorzystać rozwiązanie z połączaniem Internetowym oraz prywatnym serwerem. Zyskamy dzięki temu możliwość podglądu na aktualny stan domu, będąc w dowolnym miejscu świata. Będziemy mogli zdalnie sterować i nadzorować dowolne urządzenie podpięte do sieci naszego inteligentnego domu. W razie wystąpienia sytuacji, która wymaga naszej uwagi, system sterujący domem może wysłać powiadomienie na nasz telefon czy adres mailowy. Dodatkowo, podpięcie centrali do Internetu, pozwoli jej pobierać informacje dotyczące pogody i innych zagrożeń, a także sprawdzać dostępność aktualizacji oprogramowania dla siebie oraz innych podpiętych do niej urządzeń. Wadami tego rozwiązania są, między innymi, znacznie zwiększona ilość zagrożeń dla naszego systemu oraz ilość punktów, które mogą zostać zaatakowane i należy je zabezpieczyć. Umożliwiamy, zdalne ataki na nasz system. Do tego dochodzą koszty utrzymania serwera oraz obowiązek jego stałego monitorowania i ochrony. Jeśli natomiast, chcemy spróbować najnowszych technologi lub wprowadzamy rozwiązanie mające pomóc w nadzorowaniu i sterowaniu urządzeniami, znajdującymi się w różnych miejscach, warto przyjrzeć się usługą oferowanym przez dostawców chmury obliczeniowej. Dzięki programom ułatwiającym zarządzanie naszymi zasobami w chmurze, możemy łatwo modyfikować konfigurację. Centrala umieszczona

w chmurze jest wysoko dostępna, to znaczy odporna na awarie[1], co pozwala nam na dostęp do zawartych w niej danych przez cały czasu oraz umożliwia nam wydawanie poleceń, nawet gdy część urządzeń IoT chwilowo utraciło połączenie. Rozwiązanie to, może znacznie uprościć konstrukcję systemu, zapewnia mu większe bezpieczeństwo fizyczne oraz wsparcie od dostawcy usługi chmurowej. Jednakże, używanie tych technologii wymaga specjalistycznej wiedzy, a ze względu na to, że są one nowe i wciąż są w fazie rozwoju, brakuje ludzi, którzy wybitnie znają się na tym temacie. Dodatkowo, utrata połączenia pomiędzy centralą w chmurze, a domem pozostawia, znajdujące się w budynku, urządzenia bez nadzoru. Ponadto, wykradzenie naszych poświadczeń, może skończyć się dla nas bardzo wysokim rachunkiem[63].

Jak widać, najlepszym podejściem wydaje się uświadomienie sobie, że „żaden system nie jest bezpieczny"[64]. Przy wyborze konkretnego rozwiązania, dla naszego domu, powinniśmy odpowiedzieć sobie na pytanie, jakie funkcjonalności są dla nas najważniejsze, a następnie wybrać rozwiązania, które je zapewniają, z uwzględnieniem zabezpieczeń, które będziemy musieli wprowadzić, gdy na dane rozwiązanie się zdecydujemy. Dodatkowo, należy pamiętać, że przedstawiona w poprzednim rozdziale lista zagrożeń nie jest pełna. Część z zagrożeń zauważa sie dopiero po pewnym czasie pracy z danym rozwiązaniem, dlatego ważne jest, abyśmy cyklicznie wracali do analizowania możliwych zagrożeń dla naszego systemu i zabezpieczali go przed nimi.

[1]Awarie związane z brakiem dostępu do usług, np. odcięcie zasilania czy Internetu.

Bibliografia

[1] The number of smart homes in Europe and North America tops 17.9 million in 2015 [dostęp: 2 stycznia 2018] https://www.iot-now.com/2016/05/31/47936-the-number-of-smart-homes-in-europe-and-north-america-tops-17-9-million-in-2015/

[2] Why 2017 will finally be the year of the smart home: Consumers figure it out [dostęp: 14 stycznia 2018] https://www.cnbc.com/2017/01/04/why-2017-will-finally-be-the-year-of-the-smart-home-consumers-figure-it-out.html

[3] Stanisław Lem, *Tragedia pralnicza*, ze zbioru *Dzienniki gwiazdowe*, Wydawnictwo Literackie, 1966

[4] serial „Mr. Robot" odcinek „1 - eps2.0_unm4sk-pt1.tc", twórca Sam Esmail, 2015 - serial wciąż trwa

[5] Obcy język polski: Inteligentne (urządzenie) [dostęp: 6 stycznia 2018] https://obcyjezykpolski.pl/inteligentne-urzadzenie/

[6] Smart Lua Scripts [dostęp: 6 stycznia 2018] https://www.domoticz.com/wiki/Smart_Lua_Scripts

[7] Przykładowa aplikacja mobilna pozwalająca na dodawanie reguł do systemu „GetSafe Home Security" [dostęp: 6 stycznia 2018] https://play.google.com/store/apps/details?id=com.getsafe.homesecurity, strona producenta: [dostęp: 6 stycznia 2018] https://getsafe.com/app-overview/

[8] Przykładowy projekt „smart-home" z użyciem Arduino jako centralki. [dostęp: 6 stycznia 2018] http://www.instructables.com/id/Smart-home-with-arduino/

[9] The House That Learns: Bringing Artificial Intelligence Into The Home [dostęp: 6 stycznia 2018] https://www.forbes.com/sites/freddiedawson/2016/05/24/the-house-that-learns-bringing-artificial-intelligence-into-the-home/#64e7a5cc3fa3

[10] OK, House. Get Smart: Make the Most of Your AI Home Minions [dostęp: 6 stycznia 2018] https://www.wired.com/2017/06/guide-to-ai-artificial-intelligence-at-home/

[11] Zagrożenie - Wikipedia [dostęp: 14 stycznia 2018] https://pl.wikipedia.org/wiki/Zagro%C5%BCenie

[12] Definitions of vulnerability - Wikipedia [dostęp: 14 stycznia 2018] https://en.wikipedia.org/wiki/Vulnerability_(computing)#Definitions

[13] Project Zero - Reading privileged memory with a side-channel [dostęp: 15 stycznia 2018] https://googleprojectzero.blogspot.pt/2018/01/reading-privileged-memory-with-side.html

[14] Meltdown and Spectre [dostęp: 15 stycznia 2018] https://meltdownattack.com/#faq-systems-meltdown

[15] AAA - Wikipedia [dostęp: 6 lutego 2018] https://en.wikipedia.org/wiki/AAA_protocol

[16] RADIUS AAA [dostęp: 6 lutego 2018] http://networkradius.com/radius-aaa/index.html

[17] Authentication vs. Authorization [dostęp: 6 lutego 2018] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff687657(v=ws.10)

[18] Safety vs. Security: Understanding the Difference May Soon Save Lives [dostęp: 28 stycznia 2018] https://www.linkedin.com/pulse/20140831152519-11537006-understanding-the-difference-may-soon-save-lives-safety-vs-security

[19] Internet Rzeczy - Wikipedia [dostęp: 27 stycznia 2018] https://pl.wikipedia.org/wiki/Internet_rzeczy

[20] Internet of Things - Gartner IT Glossary [dostęp: 6 lutego 2018] https://www.gartner.com/it-glossary/internet-of-things/

[21] Internet Coke Machine [dostęp: 27 stycznia 2018] http://knowyourmeme.com/memes/internet-coke-machine

[22] The Internet Toaster [dostęp: 27 stycznia 2018] https://www.livinginternet.com/i/ia_myths_toast.htm

[23] Trojan Room coffee pot - Wikipedia [dostęp: 27 stycznia 2018] https://en.wikipedia.org/wiki/Trojan_Room_coffee_pot

[24] That „Internet of Things" Thing [dostęp: 27 stycznia 2018] http://www.rfidjournal.com/articles/view?4986

[25] Threat Risk Modeling [dostęp: 14 stycznia 2018] https://www.owasp.org/index.php/Threat_Risk_Modeling

[26] The STRIDE Threat Model [dostęp: 14 stycznia 2018] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[27] Threat Risk Modeling - STRIDE [dostęp: 14 stycznia 2018] https://www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE

[28] Chapter 2 - Threats and Countermeasures [dostęp: 16 stycznia 2018] https://msdn.microsoft.com/en-us/library/ff648641.aspx

[29] A Loud Sound Just Shut Down a Bank's Data Center for 10 Hours [dostęp: 2 lutego 2018] https://motherboard.vice.com/en_us/article/8q8dqg/a-loud-sound-just-shut-down-a-banks-data-center-for-10-hours

[30] Applying STRIDE [dostęp: 22 stycznia 2018] https://msdn.microsoft.com/en-us/library/ee798544(v=cs.20).aspx

[31] Modbus - Wikipedia [dostęp: 22 stycznia 2018] https://pl.wikipedia.org/wiki/Modbus

[32] Zigbee - Wikipedia [dostęp: 23 stycznia 2018] https://en.wikipedia.org/wiki/Zigbee

[33] Carrier-sense multiple access with collision avoidance - Wikipedia [dostęp: 6 lutego 2018] https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance

[34] Why Does Running My Microwave Kill My Wi-Fi Connectivity? [dostęp: 24 stycznia 2018] https://www.howtogeek.com/171869/why-does-running-my-microwave-kill-my-wi-fi-connectivity/

[35] Przykładowe urządzenie zagłuszające WiFi i nie tylko dostępne za 620$ [dostęp: 24 stycznia 2018] https://www.jammer-store.com/titan-all-in-one-jamming-solution.html

[36] Gotowe rozwiazanie do przeprowadzania ataku deautoryzacji i innych w sieciach bezprzewodowych z użyciem ESP8266 [dostęp: 24 stycznia 2018] https://github.com/spacehuhn/esp8266_deauther

[37] Moduł ESP8266 - AliExpress [dostęp: 24 stycznia 2018] https://www.aliexpress.com/item/Free-shipping-ESP8266-serial-WIFI-wireless-module-wireless-transceiver/32341788594.html

[38] WiFi Jammers vs Deauthers | What's The Difference? - YouTube [dostęp: 24 stycznień 2018] https://www.youtube.com/watch?v=6m2vY2HXU60

[39] WAGO I/O System [dostęp: 28 stycznia 2018] http://www.wago.pl/produkty/katalog-produktow/?id=2102418

[40] Miniserver - Loxone [dostęp: 28 stycznień 2018] https://shop.loxone.com/enuk/miniserver.html

[41] Infrastruktura klucza publicznego - Wikipedia [dostęp: 6 lutego 2018] https://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego

[42] Single-board computer - Wikipedia [dostęp: 28 stycznień 2018] https://en.wikipedia.org/wiki/Single-board_computer

[43] Arduino Uno R3 - AliExpress [dostęp: 28 stycznień 2018] https://pl.aliexpress.com/item/high-quality-One-set-UNO-R3-CH340G-MEGA328P-for-Arduino-UNO-R3-NO-USB-CABLE/32697443734.html

[44] Raspberry Pi 3 model B WiFi Bluetooth 1GB RAM 1,2GHz [dostęp: 29 stycznia 2018] https://botland.com.pl/moduly-i-zestawy-raspberry-pi-3/5576-raspberry-pi-3-model-b-wifi-bluetooth-1gb-ram-12ghz.html

[45] Specyfikacja Raspberry Pi Model B3 - Wikipedia [dostęp: 29 stycznia 2018] https://pl.wikipedia.org/wiki/Raspberry_Pi#Specyfikacja

[46] Domoticz [dostęp: 29 stycznia 2018] https://domoticz.com/

[47] OpenHUB [dostęp: 29 stycznia 2018] http://www.openhab.org/

[48] Przykładowa realizacja rozwiązania inteligentnego domu wykonana przez firmę IQ Building [dostęp: 29 stycznia 2018] http://iq-building.com/realizations/dom+320m2+-+krak%25C3%25B3w

[49] AWS IoT Core Pricing [dostęp: 29 stycznia 2018] https://aws.amazon.com/iot-core/pricing/

[50] Invoking Lambda Functions - AWS Documentation [dostęp: 6 lutego 2018] https://docs.aws.amazon.com/lambda/latest/dg/invoking-lambda-functions.html

[51] Cloud Functions Overview - GCP Documentation [dostęp: 6 lutego 2018] https://cloud.google.com/functions/docs/concepts/overview

[52] What is an IoT Gateway and How Do I Keep It Secure? [dostęp: 29 stycznia 2018] https://www.globalsign.com/en/blog/what-is-an-iot-gateway-device/

[53] AWS Free Tier (Non-expiring Offers) [dostęp: 29 stycznia 2018] https://aws.amazon.com/free/?awsf.undefined=categories%23alwaysfree

[54] Google Cloud Platform Free Tier - Always Free [dostęp: 29 stycznia 2018] https://cloud.google.com/free/

[55] Samsung TVs Hit By Killer Software Update [dostęp: 30 stycznia 2018] https://www.forbes.com/sites/johnarcher/2017/08/24/samsung-tvs-hit-by-killer-software-update/#3f5629cb7c58

[56] Smart locks rendered dumb by automatic update fail [dostęp: 30 stycznia 2018] https://www.engadget.com/2017/08/15/smart-lock-update-fail/

[57] Stunnel - About [dostęp: 3 lutego 2018] https://www.stunnel.org/

[58] OpenBSD manual - SSH [dostęp: 3 lutego 2018] https://man.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man1/ssh.1

[59] Control High Voltage Devices - Arduino Relay Tutorial [dostęp: 6 lutego 2018] http://howtomechatronics.com/tutorials/arduino/control-high-voltage-devices-arduino-relay-tutorial/

[60] What Is Input Validation and Sanitization? [dostęp: 6 lutego 2018] http://download.oracle.com/oll/tutorials/SQLInjection/html/lesson1/les01_tm_ovw3.htm

[61] Schemat przedstawiający połącznie urządzeń IoT z AWS IoT Core https://d1.awsstatic.com/IoT/diagrams/AWS%20IoT%20Core%20Authenticate.a04e344921f6ba4aedb30f356d320b1fbb4c1c07.png

[62] Service-level agreement - Wikipedia [dostęp: 6 lutego 2018] https://en.wikipedia.org/wiki/Service-level_agreement

[63] My AWS account was hacked and I have a $50,000 bill [...] [dostęp: 6 lutego 2018] https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how-can-I-reduce-the-amount-I-need-to-pay

[64] Baran bo Odar, Who Am I - Kein System ist sicher (*Who Am I - No System is safe*), Niemcy, 2014.