Table of Contents

1. Sprzęt IoT, a Cyberbezpieczeństwo 2
1.1. Podatności sprzętu IoT 2
1.2. Ataki na sprzęt IoT 3
1.3. Bezpieczeństwo sprzętu IoT 5

1. Sprzęt IoT, a Cyberbezpieczeństwo

Typowa architektura IoT składa się z warstwy fizycznej obejmującej czujniki i elementy wykonawcze IoT, które mogą być połączone w topologii gwiazdy, liniowej, siatki lub drzewa. Urządzenia IoT mogą przetwarzać dane zebrane przez czujniki w warstwie fizycznej lub przesyłać je do analizy w warstwach obliczeniowych mgły/chmury za pośrednictwem sieci dostępowych IoT i sieci szkieletowych Internetu. Węzły obliczeniowe mgły/chmury wykonują na danych lekką lub zaawansowaną analitykę, a wynik może zostać przesłany użytkownikom w celu podjęcia decyzji lub elementom wykonawczym IoT w celu wykonania określonego zadania bądź sterowania danym systemem lub procesem. Oznacza to, że w infrastrukturze IoT mogą występować urządzenia IoT, bezprzewodowe punkty dostępowe, bramy, węzły obliczeniowe mgły, routery i przełączniki internetowe, telekomunikacyjne urządzenia transmisyjne, stacje bazowe sieci komórkowych, serwery, bazy danych, węzły obliczeniowe chmury, aplikacje mobilne i aplikacje webowe. Wszystkie te urządzenia i aplikacje stanowią powierzchnię ataku, którą cyberprzestępcy mogą wykorzystać do kompromitacji urządzeń IoT.

Przy wdrażaniu bezpieczeństwa IoT należy uwzględnić rodzaj sprzętu występującego w systemach IoT – od poziomu urządzeń, przez sieci IoT, węzły obliczeniowe mgły i sieci szkieletowe Internetu, aż po chmurę. Zabezpieczenie tradycyjnej infrastruktury internetowej i chmurowej jest bardzo złożone, ale mniej problematyczne, ponieważ dysponuje się ogromnymi zasobami obliczeniowymi i komunikacyjnymi do obsługi algorytmów i aplikacji cyberbezpieczeństwa, służących do usuwania podatności oraz wykrywania i zapobiegania cyberatakom w celu zapewnienia poufności, integralności i dostępności danych i systemów. W przypadku urządzeń IoT zasoby obliczeniowe i komunikacyjne są bardzo ograniczone ze względu na ograniczoną ilość energii zasilającej urządzenie. Dlatego energochłonne i kosztowne obliczeniowo algorytmy i aplikacje cyberbezpieczeństwa nie mogą być stosowane do zabezpieczania węzłów IoT. To ograniczenie sprzętowe czyni urządzenia IoT podatnymi na cyberataki i łatwymi do skompromitowania.

1.1. Podatności sprzętu IoT

Ze względu na charakter sprzętu IoT urządzenia te są podatne na określone rodzaje ataków. Do podatności lub słabości wynikających z ograniczeń sprzętowych IoT należą m.in.:

- Poufność i integralność wrażliwych danych zbieranych przez czujniki mogą zostać łatwo naruszone z powodu braku odpowiednich zabezpieczeń lub stosowania słabych algorytmów kryptograficznych. Ze względu na ograniczone zasoby obliczeniowe urządzeń IoT trudno jest wdrożyć silne algorytmy kryptograficzne, trudne do złamania przez cyberprzestępców. Urządzenia IoT wykorzystują do obliczeń mikrokontrolery, które nie są w stanie obsłużyć silnych, ale kosztownych obliczeniowo algorytmów kryptograficznych. Czyni to urządzenia IoT podatnymi na ataki typu man-in-the-middle, w których cyberprzestępcy przechwytują i analizują bezprzewodny ruch IoT, jeśli nie jest on zaszyfrowany lub używany jest słaby schemat szyfrowania.
- Część podatności urządzeń IoT wprowadzają ich producenci. Często koncentrują się oni na minimalizacji kosztów urządzeń i czasu wprowadzenia na rynek, poświęcając niewiele uwagi wymaganiom bezpieczeństwa lub potrzebom klientów – czasem dlatego, że klienci zwracają uwagę głównie na cenę, łatwość obsługi i funkcjonalność. W efekcie urządzenia bywają dostarczane z domyślnymi hasłami, bez zaimplementowanych algorytmów szyfrowania, a niekiedy bez jakichkolwiek mechanizmów uwierzytelniania. To czyni je podatnymi na ataki.

- W niektórych wdrożeniach IoT urządzenia współdzielą te same kanały komunikacyjne, co czyni je podatnymi na ataki kolizji pakietów, w których skompromitowane urządzenia IoT wywołują kolizje pakietów w kanale, zmuszając urządzenia do szybkiego wyczerpywania zgromadzonej energii i ostatecznie do wyłączenia.
- Ponieważ komunikacja między urządzeniami IoT oraz między urządzeniami a punktem dostępowym lub bramą odbywa się w bezprzewodowych kanałach radiowych, urządzenia IoT są podatne na ataki zagłuszające (ang. *jamming*), mające na celu wymuszenie szybkiego wyczerpania zgromadzonej energii.
- Urządzenia IoT są również podatne na ataki zalewowe (ang. *flooding*), polegające na zasypywaniu ich nieszkodliwymi lub bezużytecznymi pakietami, tak aby zużywały więcej energii na ich przetwarzanie, szybko wyczerpując zapas energii i ostatecznie się wyłączając.
- Ponieważ urządzenia IoT stosunkowo łatwo zainfekować złośliwym oprogramowaniem, są one podatne na ataki, w których atakujący infekuje urządzenie malware, zmuszający je do wykonywania dodatkowych obliczeń, co szybko wyczerpuje zgromadzoną energię i ostatecznie prowadzi do wyłączenia urządzenia.
- Innym rodzajem podatności sprzętu IoT jest zatruwanie tras (ang. *route poisoning*), w którym atakujący tworzy pętle routingu, zamienia niektóre urządzenia w „czarne dziury” (ang. *sinkhole*) lub wydłuża ścieżki routingu, zmuszając urządzenia do zużywania większej ilości energii i ostatecznie do jej wyczerpania, co skraca czas życia części urządzeń w sieci.
- Urządzenia IoT można łatwo zainfekować i przekształcić w botnety, które następnie mogą posłużyć do przeprowadzania zaawansowanych ataków na dużą skalę, np. rozproszonych ataków odmowy usługi, zdolnych sparaliżować zasoby IT (serwery i bramy).
- Kolejną podatnością sprzętu IoT jest brak widoczności. Wiele urządzeń IoT jest wdrażanych bez odpowiednich identyfikatorów (adresów IP), co tworzy „martwe pola”, ponieważ urządzenia te nie są widoczne dla narzędzi monitorowania bezpieczeństwa i mogą zostać wykorzystane. Ponadto różne urządzenia mogą korzystać z różnych protokołów, co utrudnia monitorowanie wszystkich urządzeń w sieci i czyni je słabymi punktami.
- Nieskuteczny mechanizm weryfikacji oprogramowania układowego (firmware'u) umożliwia jego modyfikację lub inżynierię wsteczną, co czyni urządzenie podatnym na ataki. Atakujący mogą bezprawnie zaktualizować firmware urządzenia lub go zmodyfikować, aby łatwo przejąć nad nim kontrolę i wykorzystać je do dalszych ataków.
- Wskutek niewłaściwych strategii zarządzania urządzeniami niektóre organizacje lub osoby nie dbają o odpowiednie zabezpieczenie części urządzeń (nie instalują niezbędnych aktualizacji i nie łatają luk bezpieczeństwa), pozostawiając je podatnymi na ataki cyberprzestępców.
- Niektóre podatności sprzętowe są trudne do wyeliminowania, np. ataki kanałem bocznym, inżynieria wsteczna sprzętu, infekcje złośliwym oprogramowaniem i wydobywanie danych, które mogą zostać wykorzystane i doprowadzić do naruszenia ochrony danych.
- Urządzenia IoT są podatne na ataki fizyczne. Przestępca może je zniszczyć, uszkodzić, a nawet uzyskać do nich bezpośredni dostęp.

1.2. Ataki na sprzęt IoT

Ataki na sprzęt IoT to różne sposoby wykorzystania słabości bezpieczeństwa wynikających z ograniczeń sprzętu IoT w celu naruszenia bezpieczeństwa danych i systemów IoT. Atakujący może zainstalować na urządzeniach IoT złośliwe oprogramowanie, zmanipulować ich działanie lub wykorzystać ich słabości, aby uzyskać dostęp i ukraść lub zniszczyć dane, obniżyć jakość usług lub je zakłócić. Atakujący może zaatakować urządzenia IoT po to, by wykorzystać je do bardziej zaawansowanego ataku na dużą skalę na infrastrukturę ICT i systemy krytyczne. Skala i częstotliwość ataków na IoT rosną ze względu na powiększającą się powierzchnię ataku IoT, łatwość kompromitacji

urządzeń IoT oraz ich integrację z istniejącymi systemami i infrastrukturą krytyczną. Do typowych ataków na sprzęt IoT należą:

- Nieuprawniony dostęp: niektórzy producenci urządzeń IoT stosują słabe mechanizmy bezpieczeństwa lub nie stosują ich wcale, aby zminimalizować koszty produkcji i skrócić czas wprowadzenia produktu na rynek w odpowiedzi na rosnący popyt. Czasem nie zapewniają mechanizmów niezbędnych do aktualizacji i łatania luk w zabezpieczeniach. Niektórzy tworzą tylne furtki do zdalnego serwisowania, które mogą wykorzystać hakerzy, inni zaś stosują hasła domyślne lub nie stosują ich wcale, co ułatwia atakującym dostęp do urządzenia i wykorzystanie go do eskalacji ataków.
- Emulacja fałszywych urządzeń IoT: strona trzecia znająca protokół komunikacyjny może opracować oprogramowanie emulujące standardowe funkcje urządzeń IoT, a następnie wykorzystać je do rozpowszechniania fałszywych informacji.
- Kradzież tożsamości: atakujący może przejąć tożsamość legalnego urządzenia, a następnie wykonywać złośliwe działania w sieci, pozostając niezidentyfikowanym.
- Wstrzykiwanie fałszywych informacji: atakujący może wprowadzać fałszywe lub wprowadzające w błąd informacje, aby zakłócić zamierzone działanie systemu. Na przykład w łańcuchu dostaw żywności strona trzecia mogłaby wprowadzić fałszywe odczyty czujnika etylenu, przez co system uznałby, że transportowany towar jest już zepsuty. Dlatego należy wdrożyć mechanizmy chroniące system przed wstrzykiwaniem fałszywych informacji.
- Ataki na firmware: po wykryciu nowego zagrożenia bezpieczeństwa wymagana jest aktualizacja firmware'u, aby uzyskać wersję usuwającą to zagrożenie. Firmware, konfiguracja zabezpieczeń i inne cechy urządzenia mogą zostać sklonowane. Atakujący może również zaktualizować firmware urządzenia złośliwym oprogramowaniem [1)].
- Podsłuch i ataki man-in-the-middle: wymiana danych powinna odbywać się w sposób bezpieczny, uniemożliwiający ich przechwycenie przez strony trzecie. W urządzeniach IoT nie można stosować tradycyjnych schematów szyfrowania – wymagają one szyfrowania lekkiego, którego wdrożenie nie jest proste i bywa pomijane przez producentów. Przesyłanie niezaszyfrowanych danych IoT, w tym danych bezpieczeństwa, czyni sieci IoT podatnymi na podsłuch i ataki typu man-in-the-middle.
- Ataki wyczerpujące energię: atakujący dąży do znacznego zwiększenia zużycia energii przez zasilane bateryjnie urządzenie IoT, wyczerpania jego baterii i ostatecznie wyłączenia urządzenia. Przykładami takich ataków są Denial of Sleep (DoS), flooding, ataki karuzelowe (ang. *carousel*) i rozciągające (ang. *stretch*) [2)].
- Ataki wampirze (ang. *vampire attacks*): atakujący dąży do znacznego zwiększenia zużycia energii przez zasilane bateryjnie urządzenie IoT, wyczerpania jego baterii i ostatecznie wyłączenia urządzenia. Przykładami takich ataków są Denial of Sleep (DoS), flooding, ataki karuzelowe i rozciągające [3)].
- Ataki na routing: atakujący może manipulować informacjami o routingu urządzeń, aby tworzyć pętle routingu, selektywnie przekazywać pakiety lub wymuszać dłuższe trasy, co zwiększa zużycie energii. Do ataków na routing należą m.in. sinkhole, selektywne przekazywanie (ang. *selective forwarding*), wormhole i atak Sybilli [4)].
- Ataki zagłuszające (ang. *jamming*): atak odmowy usługi we współdzielonym kanale komunikacji bezprzewodowej, w którym jeden użytkownik uniemożliwia innym korzystanie ze współdzielonego kanału [5)]. Jest to atak na warstwę fizyczną lub warstwę łącza danych bezprzewodowej sieci IoT.
- Ataki siłowe (brute-force): ich celem jest zdobycie danych logowania w celu uzyskania nieuprawnionego dostępu do urządzenia. W przypadku urządzeń z hasłami domyślnymi, powszechnie używanymi (np. admin) lub słabymi, atakujący mogą zdobyć te dane i wykorzystać je do nielegalnego dostępu do urządzeń IoT.
- Ataki DoS/DDoS: ponieważ nie wdraża się odpowiednich mechanizmów wzmacniających

bezpieczeństwo urządzeń IoT, można je łatwo skompromitować. Wiele urządzeń IoT może utworzyć armię botnetów przeprowadzających ataki DDoS, które wyczerpują bufory i inne zasoby punktów dostępowych, węzłów mgły i platform chmurowych.
- Ataki kolizji pakietów: atak typowy dla zastosowań IoT, w których urządzenia współdzielą bezprzewodowy kanał komunikacyjny. Atakujący może przejąć część urządzeń i wykorzystać je do wywoływania kolizji pakietów w kanale, aby zakłócić komunikację i zmusić urządzenia do zużywania większej ilości energii na wielokrotne retransmisje oraz wydłużyć czas, w którym pozostają aktywne (czyli skrócić czas uśpienia). Jest to odmiana ataku wyczerpującego energię.
- Fizyczny atak na urządzenie: urządzenie IoT może zostać fizycznie zmanipulowane lub uszkodzone w celu wydobycia kluczowych informacji. Jest to istotne np. w rolnictwie opartym na IoT, gdzie infrastruktura IoT na polach może zostać zniszczona.

1.3. Bezpieczeństwo sprzętu IoT

Wyeliminowanie podatności sprzętu IoT jest bardzo trudne ze względu na ograniczone zasoby sprzętowe urządzeń IoT. Do środków zabezpieczania urządzeń IoT i ograniczania ryzyka wynikającego z ich podatności należą m.in.:

- Wdrożenie lekkich schematów szyfrowania w urządzeniach IoT: dane przechowywane w urządzeniach IoT (np. dane uwierzytelniające urządzenia i inne dane wrażliwe) powinny być szyfrowane, aby chronić ich poufność i integralność. Dane IoT powinny być szyfrowane przed przesłaniem przez jakiekolwiek medium transmisyjne. Ponieważ tradycyjne algorytmy kryptograficzne są kosztowne obliczeniowo i wymagają wydajnych, energochłonnych systemów obliczeniowych, zaleca się stosowanie lekkich algorytmów kryptograficznych zużywających stosunkowo mniej energii.
- Wdrożenie solidnych mechanizmów uwierzytelniania w urządzeniach IoT: należy wdrożyć solidne mechanizmy uwierzytelniania, aby ograniczyć dostęp do urządzeń IoT i zapewnić, że wszystkie urządzenia łączące się z punktami dostępowymi i serwerami są uwierzytelnione. Pozwala to kontrolować dostęp do krytycznych zasobów, takich jak punkty dostępowe, bramy i serwery, oraz zapewnić autentyczność komunikacji. Ważne jest również unikanie zakupu urządzeń z hasłami wbudowanymi na stałe, zmiana haseł domyślnych i tworzenie silnych haseł do urządzeń.
- Konfiguracja zapór sieciowych chroniących urządzenia przed atakami wykorzystującymi ruch sieciowy: perymetr sieci można chronić zaporami odrzucającymi złośliwy ruch na brzegu sieci, tzn. przepuszczającymi wyłącznie ruch z legalnych źródeł i blokującymi ruch ze źródeł uznanych za złośliwe. Zapory mogą też służyć do segmentacji sieci, tak aby sieć IoT była odizolowana od innych sieci, a ataki na nią nie mogły rozprzestrzeniać się na inne. Na poszczególnych urządzeniach można skonfigurować zapory programowe, które ograniczają ruch z nieautoryzowanych źródeł.
- Zapewnienie, że komponenty programowe i sprzętowe nie są skompromitowane: komponenty programowe i sprzętowe stosowane w urządzeniach IoT powinny być dokładnie przetestowane, aby nie zawierały podatności, których atakujący mogliby użyć do naruszenia bezpieczeństwa danych i urządzeń. Środki bezpieczeństwa powinny być uwzględnione na każdym etapie cyklu życia urządzenia, tak aby znane podatności zostały usunięte, a strategie bezpieczeństwa chroniły urządzenie i dane.
- Zastosowanie dedykowanego sprzętu bezpieczeństwa: dedykowane komponenty sprzętowe są projektowane specjalnie do realizacji funkcji związanych z bezpieczeństwem (np. bezpiecznej komunikacji, energooszczędnych funkcji kryptograficznych i zarządzania kluczami), co zapewnia bezpieczeństwo urządzeń w czasie rzeczywistym. Niektóre z nich ułatwiają wdrożenie

bezpiecznego rozruchu (ang. *secure boot*) i operacji uwierzytelniania. Dodatkową zaletą dedykowanego sprzętu bezpieczeństwa IoT jest to, że część takich rozwiązań projektuje się z myślą o równowadze między ograniczeniami sprzętowymi, zużyciem energii i bezpieczeństwem.
- Każdorazowa weryfikacja poprawności i wiarygodności oprogramowania i firmware'u urządzeń IoT: należy wdrożyć niezawodne mechanizmy weryfikacji poprawności i wiarygodności oprogramowania oraz firmware'u urządzeń IoT. Pozwala to sprawdzić, czy oprogramowanie lub system operacyjny urządzenia nie zostały zmodyfikowane w sposób, który czyni je podatnym na ataki.
- Regularne kontrole bezpieczeństwa i aktualizacje: należy wdrożyć mechanizmy sprawdzania, czy urządzenie nie zostało zmodyfikowane. Firmware i oprogramowanie urządzenia powinny być regularnie aktualizowane w celu łatania luk bezpieczeństwa.
- Regularne audyty bezpieczeństwa: sieć IoT powinna być regularnie audytowana z użyciem narzędzi do skanowania podatności i audytu bezpieczeństwa, aby podatności IoT (w tym sprzętowe) i zagrożenia były wykrywane i usuwane, zanim wykorzystają je przestępcy.
- Egzekwowanie polityk bezpieczeństwa: należy opracować i egzekwować przemyślane polityki bezpieczeństwa tak, aby urządzenia i dane IoT nie były łatwe do skompromitowania. Przykładem jest stosowanie zasady *security by design* przy projektowaniu i wdrażaniu sprzętu i oprogramowania IoT. Wszystkie urządzenia IoT muszą być identyfikowalne, stale monitorowane i regularnie audytowane, aby znane podatności były usuwane na czas. Ataki na urządzenia IoT również powinny być wykrywane i blokowane na czas.

1)

O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen, R. Struik, Security Considerations in the IP-based Internet of Things draft-garcia-core-security-06, Internet Engineering Task Force (IETF), https://tools.ietf.org, 2013 accessed on 28/02/2020.

2)

A. Rayes, S. Salam, Internet of Things-From Hype to Reality, Springer Nature, 2017.

3) , 4)

A. Rayes, S. Salam, Internet of Things-From Hype to Reality, Springer Nature, 2017.

5)

S. Yan-Qiang, W. Xiao-dong, Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, DOI: 10.4018/978-1-61520-701-5.ch015, IGI Global Knowledge Disseminator, https://www.igi-global.com/chapter/jamming-attacks-countermeasures-wireless-sensor/41122, 2010, access date: 7/03/2020

From:
https://dokuwiki.zmitac.aei.polsl.pl/ - **RAU6 Dokuwiki**

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures:hardware_and_cybersecurity

Last update: **2026/11/01 15:07**