Wprowadzenie

Przedsiębiorstwa komercyjne, instytucje rządowe i wojskowe coraz częściej padają ofiarą cyberataków, których celem jest kradzież poufnych informacji lub zakłócanie działania usług. Ze względu na konieczność zintegrowania w przyszłych działaniach wielu dziedzin i zapewnienia odporności na wysoką sporność cyberprzestrzeni, istnieje pilne zapotrzebowanie na rozwiązania z dziedziny cyberbezpieczeństwa, które zapewnią identyfikowalność, widoczność manipulacji, rozliczalność oraz audytowalność danych dowódczych, logistycznych i innych danych kluczowych dla działalności informacji. Stąd bierze się też potrzeba skupienia się na takich rozwiązaniach z dziedziny cyberbezpieczeństwa, które będą mogły zapewnić niezawodne działanie systemów podczas podejmowanych przez przeciwników ataków. Istniejące rozwiązania w tym zakresie są rozwiązaniami reaktywnymi i nie są w stanie poradzić sobie z gwałtownym wzrostem liczby cyberzagrożeń. Scentralizowane, czyli homogeniczne systemy informatyczne i bazy danych muszą ewoluować w stronę rozproszonych, bezpośrednich i bezpiecznych systemów.

Strategia cyberobrony sprowadzać się będzie do zapewnienia zdolności operowania na danych w bezpiecznym i zaufanym środowisku. Aby wygrać w walce cybernetycznej, wojsko musi zabezpieczyć swoje operacje na danych przez: (i) zapobieganie dostępowi przeciwników do sieci zawierających krytyczne dane, (ii) zapewnienie integralności danych mimo obecności przeciwników w sieci, oraz (iii) osiągnięcie odporności na próby manipulacji danymi podejmowane przez przeciwników. Jednocześnie rozwój technologii chmury i Internetu rzeczy, które wspierają usługi przetwarzania na żądanie (*on-demand computing*), dynamiczną aprowizację i zarządzanie systemami autonomicznymi, zwiększa potrzeby w zakresie poprawy ich bezpieczeństwa. Kluczowym zagadnieniem jest zapewnienie bezpieczeństwa zarządzania i przesyłania danych wewnątrz środowisk chmury i między takimi środowiskami. Audyt środowisk chmurowych będzie skuteczny tylko wtedy, gdy można będzie wiarygodnie prześledzić wszystkie operacje wykonywane na danych, czyli zebrać informacje o pochodzeniu danych, które pomogą w wykrywaniu włamań w infrastrukturach chmury obliczeniowej. Internet rzeczy (IoT) w kontekście

wojskowym umożliwia łączenie ze sobą zasobów bojowych, takich jak czujniki, amunicja, broń, pojazdy, roboty i urządzenia ubieralne, umożliwiając realizację takich zadań, jak wykrywanie, komunikacja, współdziałanie i współpraca z żołnierzami. Ogromna skala i rozproszony charakter urządzeń IoT stwarzają wiele problemów związanych z bezpieczeństwem i prywatnością danych. Przede wszystkim bazowa infrastruktura sieciowa i komunikacyjna Internetu rzeczy musi być elastyczna i dostosowana do wsparcia dynamiki misji wojskowych. Ta dynamiczna zmiana infrastruktury komunikacyjnej musi się dokonać w sposób autonomiczny bez uzależniania się od scentralizowanych usług utrzymaniowych. Po drugie, należy zapewnić prawdziwość informacji udostępnianych za pośrednictwem urządzeń IoT. Stąd potrzeba opracowania zaufanej platformy, która zapewni dokładność i wierność informacji przekazywanych żołnierzom.

Blockchain oraz rozwijające się technologie rozproszonych publicznych rejestrów danych mają cechy prawdziwie rozproszonych i bezpośrednich systemów zapewniających pełną rozliczalność i audytowalność. Blockchain, czyli łańcuch bloków, to dostępna publicznie, rozproszona i odporna na uszkodzenia i modyfikacje baza danych, którą każdy uczestnik sieci może udostępniać i nad którą nikt nie może przejąć wyłącznej kontroli. Blockchainy zakładają obecność przeciwników w sieci i ich celem jest niwelowanie wrogich strategii przez wykorzystanie możliwości obliczeniowych uczciwych węzłów i zapewnienie odporności informacji przekazywanych za ich pośrednictwem na manipulacje i zniszczenie. Ta zdolność pozwala dowodzącym kontynuować działania wojskowe mimo działań podejmowanych przez przeciwników. Rozwiązania kwestii cyberbezpieczeństwa oparte na blockchainie będą stanowić zmianę paradygmatu w sposobie zabezpieczania się przed manipulacją danymi. Blockchain umożliwia budowanie zaufanych systemów w środowiskach pozbawionych zaufania. Manipulowanie łańcuchami bloków staje się w nich niezwykle trudne ze względu na zastosowanie kryptograficznych struktur danych i założenie braku zaufania. Blockchain umożliwia wzmocnienie cyberobrony dzięki swojej zdolności do zapobiegania nieautoryzowanym działaniom w oparciu o mechanizm rozproszonego konsensusu, a także dzięki zapewnianiu integralności danych przez swoją niemodyfikowalność, możliwości audytu i mechanizmy odporności operacyjnej (czyli brak pojedynczego słabego ogniwa powodującego rozległą awarię systemu). Chociaż blockchain nie jest panaceum na wszystkie problemy cyberbezpieczeństwa, to technologia ta może pomóc organizacjom w rozwiązywaniu problemów z dziedziny cyberbezpieczeństwa, takich jak zarządzanie tożsamością, zapewnianie informacji o pochodzeniu danych i zapewnianie integralności danych.

Książka ta poświęcona jest zastosowaniom rozwiązań opartych na blockchainie w systemach rozproszonych tworzących odporną i niezawodną cyberinfrastrukturę wspierającą działalność i misję korzystających z niej podmiotów. Istnieje potrzeba

zrozumienia, jak blockchain może oddziaływać w sferach wykraczających poza kryptowaluty i w jaki sposób może rozwiązywać problemy bezpieczeństwa i prywatności danych w chmurach i w platformach IoT/IoBT. Tematy poruszane w tej książce dotyczą podstawowych właściwości i formalnych podstaw technologii blockchain oraz praktycznych problemów związanych z jej wdrażaniem w środowiskach chmury i na platformach IoT. Ponadto książka ta przedstawia wyzwania w zakresie bezpieczeństwa, które należy pokonać, aby technologie blockchain mogły w pełni wykazać swój potencjał. Trzy rozdziały książki (4, 5 i 8) oparte są na artykułach badawczych, które na konferencji Blockchain Connect 2019 zostały wyróżnione tytułem „Top Blockchain paper"[1].

Publikacja ta jest oparta na badaniach sponsorowanych przez Laboratorium Badawcze Sił Powietrznych Stanów Zjednoczonych (Air Force Research Laboratory), w ramach umowy nr FA8750-16-0301. Chcielibyśmy podziękować AFRL za wsparcie finansowe, współpracę i pomoc. Rząd Stanów Zjednoczonych jest upoważniony do powielania i rozpowszechniania przedruków w celach rządowych, bez względu na wszelkie zapisy dotyczące praw autorskich. Prace opisane w tej książce były również częściowo wspierane z innych źródeł, które wskazano w poszczególnych rozdziałach.

Redakcja pragnie potwierdzić wkład w powstanie tej książki następujących osób (w kolejności alfabetycznej): Abdulhamid Adebayo, Philip Asuquom, Shihan Bao, Yue Cao, Haitham Cruickshank, Ali Dorri, Peter Foytik, Arash Golchubian, Y. Thomas Hou, Raja Jurdak, Salil S. Kanhere, Kevin Kwiat, Adriaan Larmuseau, Ao Lei, Jin Li, Xueping Liang, Wenjing Lou, Andrew Miller, Aziz Mohaisen, Mehrdad Nojoumian, DaeHun Nyang, Danda B. Rawat, Muhammad Saad, Devu Manikantan Shila, Jeffrey Spaulding, Marco Steger, Zhili Sun, Deepak Tosh, Yang Xiao i Ning Zhang. Dodatkowe podziękowania kierujemy również do: Misty Blowers, Jerry'ego Clarke'a, Jima Perretta i Val Red za ich cenne wsparcie i wskazówki. Za pomoc w redakcji technicznej dziękujemy następującym osobom: Paulowi Ratazzi, Robertowi Reschly i Michaelowi Weismanowi. Na koniec przekazujemy podziękowania i wyrazy uznania dla: Jovina E. Allena, Waltera J. Baileya, Sandry B. Fletcher, Lisy M. Lacey, Sandry H. Montoya, Lorri E. Roth i Jessici D. Schultheis, którzy pomagali nam w pracach redakcyjnych i w przygotowaniu ostatecznej postaci książki. Dodatkowo dziękujemy Mary Hatcher i Vishnu Narayanan z wydawnictwa Wiley za ich uprzejmą pomoc w doprowadzeniu do publikacji tej książki.

Zastrzeżenia: Poglądy i treści wyrażone w tej książce są poglądami autorów i nie odzwierciedlają oficjalnej polityki ani stanowiska Departamentu Obrony, ani rządu Stanów Zjednoczonych.

[1] https://medium.com/blockchain-connect-conference/top-50-blockchainpapers-and-research-team-lead-you-to-the-frontier-of-blockchainacademic-277b0358b784