Ewa Niewiadomska-Szynkiewicz*
Rafał Litka**

Ataki na urządzenia mobilne i metody ich wykrywania

Streszczenie

Indywidualna ochrona systemów autonomicznych z wykorzystaniem prostej analizy przesyłanych komunikatów staje się niestety niewystarczająca. Istnieje wyraźna potrzeba stworzenia nowych rozwiązań wykorzystujących dane z wielu źródeł, integrujących różne metody, mechanizmy ialgorytmy, w tym techniki przetwarzania Big Data i klasyfikacji danych wykorzystujące metody sztucznej inteligencji. Ilość, jakość, wiarygodność i aktualność danych i informacji o sytuacji w sieci oraz szybkość ich przetwarzania decydują o skuteczności ochrony. W pracy prezentowane są przykłady wykorzystania technik sztucznej inteligencji do wykrywania ataków na systemy teleinformatyczne. Uwaga koncentruje się na zastosowaniu metod uczenia maszynowego do detekcji złośliwych aplikacji instalowanych na urządzeniach mobilnych. Skuteczność przedstawionych rozwiązań została potwierdzona przez liczne eksperymenty symulacyjne przeprowadzone na rzeczywistych danych. Uzyskano obiecujące wyniki.

Słowa kluczowe: cyberbezpieczeństwo, detekcja ataków, aplikacje mobilne, sztuczna inteligencja, uczenie maszynowe, sztuczne sieci neuronowe, głębokie uczenie

* Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz, kierownik Zespołu Złożonych Systemów, Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, e-mail: ewa.szynkiewicz@pw.edu.pl, ORCID: 0000-0003-4782-3816.
** Inż. Rafał Litka, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, e-mail: rafal.litka.stud@pw.edu.pl.

Wprowadzenie

Technologie informacyjne i komunikacyjne (ang. Information and Telecommunication Technologies – ITC) to obecnie jeden z podstawowych elementów decydujących o poziomie rozwoju społeczeństw. Intensywny rozwój sieci i systemów teleinformatycznych stymuluje rozwój nowoczesnych gałęzi przemysłu oraz nowatorskich rozwiązań w efektywnej organizacji pracy i zarządzania procesami. Z powszechnym wykorzystaniem i dynamicznym rozwojem technologii informacyjnych wiążą się, niestety zagrożenia bezpieczeństwa państw, organizacji i obywateli. Nowoczesne systemy teleinformatyczne są narażone na liczne cyberataki. Są one coraz bardziej wyrafinowane i trudniejsze do wykrycia. Celem jest zazwyczaj wykonywanie niepożądanych operacji na komputerze ofiary skutkujących m.in. dystrybucją złośliwego oprogramowania w sieci, przechwytywaniem wrażliwych informacji oraz zakłócaniem pracy.

Zespoły ds. cyberbezpieczeństwa z różnych krajów potwierdzają, że z każdym rokiem sukcesywnie wzrasta liczba incydentów i ataków w cyberprzestrzeni. W 2021 roku na podstawie 116 071 zgłoszeń zespół CERT Polska zarejestrował 29 483 unikatowe incydenty cyberbezpieczeństwa[1]. Najczęstszym typem ataku, podobnie jak w kilku ostatnich latach, były oszustwa komputerowe, które stanowiły 86,4% wszystkich obsłużonych incydentów. W stosunku do poprzedniego roku był to prawie trzykrotny wzrost. Na drugim miejscu znalazło się złośliwe oprogramowanie – 9,66% obsłużonych incydentów. Najczęściej ataki dotykały sektor mediów, handlu, poczty i usług kurierskich oraz energetyki. Zaobserwowano liczne próby wykorzystania przyzwyczajeń i nieostrożnego zachowania użytkowników sieci. Obsłużono 36 incydentów zaklasyfikowanych jako poważne, tj. takie, które mogą wpływać na świadczenie usług kluczowych. Najwięcej dotyczyło sektora bankowego.

W ostatnich latach kluczowe znaczenie ma postęp technologii mobilnych zapewniających dostęp do systemów i zasobów w dowolnym czasie i miejscu. Liczne aplikacje mobilne wspierają prowadzenie działalności gospodarczej, są stymulatorem innowacyjnych form komunikacji, prowadzą do istotnych przewartościowań w zachowaniach społecznych. Wykorzystanie elektronicznych środków komunikacji jest coraz powszechniejszą formą świadczenia pracy i kontaktów międzyludzkich. Na podstawie analiz firmy IDC[2] przewiduje się, że

1 *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2021*, Warszawa 2022.
2 https://www.idc.com/.

w Stanach Zjednoczonych w 2024 roku pracownicy mobilni będą stanowili 60% wszystkich pracowników. Nie jest zaskoczeniem gwałtownie rosnąca liczba cyberataków inicjowana przez złośliwe aplikacje mobilne lub widomości SMS.

Przeniesienie działalności do internetu oraz problemy związane z zapewnieniem bezpieczeństwa systemów komputerowych i ich użytkowników oraz niezawodnego funkcjonowania państw spowodowały podjęcie znacznych wysiłków w środowiskach nauki, administracji i biznesu. Działania te obejmują legislację, polityki i agendy dotyczące cyberbezpieczeństwa, mapy drogowe na poziomie krajowym i międzynarodowym oraz inicjowanie krajowych i międzynarodowych projektów badawczych. Wyzwaniem jest opracowanie nowych rozwiązań do skutecznej ochrony systemów komputerowych przed znanymi zagrożeniami oraz szybkiego rozpoznawania anomalii, które mogą być symptomem złośliwych działań i wykrywania nowych, nieznanych ataków. Wymaga to innowacyjnych metod i narzędzi do rozproszonego monitorowania, analizy masowych i nieustrukturyzowanych danych, klasyfikacji incydentów i wykrywania zagrożeń. Integracja danych, zaawansowane statystyki, techniki uczenia maszynowego są coraz częściej wykorzystywane do korelacji obserwowanych zdarzeń i detekcji ataków cybernetycznych.

W artykule przedstawiono przykłady potwierdzające skuteczność zastosowania metod sztucznej inteligencji do budowy systemów wykrywania złośliwego oprogramowania, konkretnie, złośliwych aplikacji mobilnych zainstalowanych na urządzeniu użytkownika. Pierwsza część pracy stanowi wprowadzenie w zagadnienia cyberbezpieczeństwa. Omawiane są popularne klasy złośliwego oprogramowania oraz metody i techniki ochrony przed atakami. Następnie uwaga koncentruje się na algorytmach uczenia maszynowego. Prezentowany jest przykład zastosowania technik sztucznej inteligencji do wykrywania złośliwych aplikacji mobilnych. Skuteczność opracowanych rozwiązań została potwierdzona przez liczne eksperymenty symulacyjne przeprowadzone na rzeczywistych danych.

Ataki komputerowe i metody obrony

Incydenty bezpieczeństwa w systemach teleinformatycznych mogą być powodowane przez zdarzenia losowe i nieumyślne działanie użytkowników lub wynikać z celowego działania osób nieuprawnionych. Ataki cybernetyczne są realizowane z wykorzystaniem różnych technik i sposobów uzyskania nieautoryzowanego dostępu do systemu komputerowego, urządzenia sieciowego,

pomiarowego czy sterującego w celu przejęcia nad nim kontroli i wydobycia informacji. W literaturze są szeroko omawiane różne wektory ataku. Ataki można klasyfikować ze względu na ich źródło, profil, cel i skutki oraz zastosowane narzędzia i techniki. Ze względu na źródło możemy wyróżnić ataki z wykorzystaniem fizycznego dostępu do urządzenia lub zdalne, wykonywane z lokalnej lub globalnej sieci. Można je przeprowadzić, wstrzykując złośliwe oprogramowanie (malicious software -- malware), wykorzystując załączniki poczty elektronicznej, specjalne strony internetowe, protokoły itd. Powstaniu sieci internet towarzyszyło pojawianie się, z czasem coraz doskonalszych i groźniejszych, odmian złośliwego oprogramowania. Różni je cel i sposób działania. Niekiedy występują łącznie, aktywując się w różnych fazach infekcji. Poniżej są wymienione przykłady najbardziej znanych klas złośliwego oprogramowania.

1. Wirus – program lub fragment kodu infekujący systemy komputerowe, dołączany do powszechnie używanych programów (nosicieli), przenoszony i powielany bez wiedzy użytkownika. Specjalna odmiana wirusa – koń trojański (tzw. trojan) – podszywa się pod użyteczne oprogramowanie i instaluje podczas pobierania programów, ściągania plików i otwierania zainfekowanych załączników.

2. Robak – samodzielny program rozprzestrzeniający się zazwyczaj za pośrednictwem sieci;

3. Exploit – program, fragment kodu lub rodzaj ataku polegający na wykorzystaniu błędów w oprogramowaniu w celu przejęcia kontroli nad komputerem użytkownika. Backdoor to celowo wprowadzona luka w systemie operacyjnym lub oprogramowaniu, która pozwala nieuprawionym osobom na obejście zabezpieczeń systemu komputerowego.

4. Ransomware – oprogramowanie blokujące dostęp do systemu lub uniemożliwiające odczytanie przechowywanych w nim danych przez założenie blokady lub zaszyfrowanie plików. Odzyskanie dostępu do systemu wymaga opłacenia okupu.

5. Spyware – oprogramowanie zbierające dane osobowe i poufne użytkownika oraz monitorujące jego aktywność, w tym przeglądane strony.

6. Keylogger – rodzaj oprogramowania śledzącego aktywność użytkownika podczas korzystania z klawiatury.

7. Rootkit – zespół programów maskujących obecność złośliwego kodu i umożliwiających włamania do systemów komputerowych.

8. Adware – oprogramowanie powodujące natrętne wyświetlanie reklam, utrudniające korzystanie z zainfekowanego urządzenia.

Celem działania złośliwego oprogramowania jest najczęściej kradzież danych, tożsamości, zasobów, zmiana ustawień sieci, instalacja fałszywych certyfikatów, deaktywacja oprogramowania zabezpieczającego przed atakami, kompromitacja wizerunku, zużycie zasobów i odmowa usługi (atak DoS – Denial of Service) itd. Często jest to zastawienie pewnej pułapki, np. fałszywej strony WWW, w celu pozyskiwania w przyszłości poufnych danych, w tym parametrów logowania do zasobów (phishing) lub przekształcenie zaatakowanego systemu w zombie (element sieci botnet), czyli przejęcie kontroli nad systemem w celu jego wykorzystania do szkodliwych działań, nieautoryzowanych przez użytkownika.

W ostatnich latach coraz częściej do przeprowadzania ataków są wykorzystywane telefony komórkowe. Ataki są inicjowane m.in. przez złośliwe aplikacje mobilne instalowane przez użytkowników i pobierane z niezaufanych źródeł lub nawet oficjalnych zasobów udostępnianych przez twórców systemów operacyjnych, np. sklep Google Play dla systemu Android. Innym sposobem są złośliwe wiadomości SMS (np. oprogramowanie Flubot) oraz e-maile zawierające linki do złośliwych aplikacji lub przekierowujące na fałszywe strony internetowe. Z badań firmy Check Point[3] wynika, że w 2021 roku 97% przedsiębiorstw miało do czynienia z atakiem na urządzenia mobilne. W 46% instytucji co najmniej jeden pracownik pobrał szkodliwą aplikację mobilną, i tym samym naraził sieć firmową na atak i ryzyko utraty informacji. Głównym źródłem ataków była sieć komputerowa. Najczęściej były to kampanie phishingowe (52%) nakłaniające użytkowników do instalacji szkodliwego oprogramowania, komunikowania się z zainfekowanym oprogramowaniem lub stronami internetowymi. Badania przeprowadzone przez firmę Check Point potwierdzają, że urządzenia mobilne są z natury podatne na ataki. Przyczyną są m.in. podatności kodu wykryte w oprogramowaniu procesorów sygnałowych firmy Qualcomm, która dostarcza układy do ponad 40% telefonów komórkowych na rynku. Wyniki prowadzonych w 2021 roku analiz prezentowane w raporcie opracowanym przez firmę Kaspersky[4] potwierdzają wykrycie 3,5 mln szkodliwych mobilnych pakietów instalacyjnych, które spowodowały 46,2 mln ataków na całym świecie i 80% tych ataków wiązało się z wykorzystaniem złośliwych aplikacji mobilnych. Wzrosła znacznie (do 2,3 mln) liczba ataków z wykorzystaniem trojanów bankowych. Eksperci firmy Kaspersky informują

3 *Mobile security report 2021*, Izrael 2022.

4 T. Shishkova, A. Kivva, *Mobile malware evolution 2021*, 21 Feb 2022, https://securelist.com/mobile-malware-evolution-2021/105876/ [dostęp: 10.01.2023].

o pojawieniu się ponad 95 tys. nowych, udoskonalonych wersji takich narzędzi. Cyberprzestępcy stawiają na jakość, koncentrują wysiłki na podnoszeniu skuteczności narzędzi ataku w celu zwiększania zysków z przestępstw komputerowych.

Powszechne stosowanie urządzeń internetu rzeczy (IoT) przyczyniło się do znacznego wzrostu zainteresowania cyberprzestępców tego typu systemami. Niezabezpieczone urządzenia pomiarowe i sterujące, tworzące systemy IoT, są wykorzystywane do prowadzenia zmasowanych ataków[5]. Najczęściej wymieniane na liście OpenWeb Application Security Project (OWASP) Top 10 Internet of Things zagrożenia to: słabe do odgadnięcia lub zakodowane hasła, niezabezpieczone usługi sieciowe, niezabezpieczony transfer i przechowywanie danych, brak aktualizacji, niewystarczająca ochrona prywatności itd. Niestety, usunięcie nawet znanych podatności jest trudne i kosztowne, gdyż często wymaga modyfikacji sprzętu i angażuje jego producenta.

Żeby sprostać dzisiejszym wymogom bezpieczeństwa i utrzymać ciągłość działania organizacji, konieczne jest zapewnienie sprawnych i skutecznych działań w celu identyfikacji i szybkiego reagowania na incydenty związane z cyberbezpieczeństwem. Systemy wykrywania włamań IDS (Intrusion Detection Systems) i systemy zapobiegania włamaniom IPS (Intrusion Prevention Systems) to części infrastruktury sieciowej wykorzystywane do ochrony sieci przed cyberatakami. Systemy IDS monitorują sieć, porównują bieżącą aktywność sieciową ze znaną bazą zagrożeń w celu wykrywania anomalii, złośliwego oprogramowania, naruszeń polityki bezpieczeństwa. Systemy IPS działają na styku sieci wewnętrznej i świata zewnętrznego. To sprzętowe lub programowe rozwiązania, których zadaniem jest uniemożliwianie przeprowadzenia ataków. Systemy IDS/IPS implementują różne architektury i metody wykrywania zagrożeń, oferują różne poziomy bezpieczeństwa[6].

Większość instytucji, zwłaszcza tych ważnych dla państwa, buduje w swoich strukturach centralne jednostki zajmujące się cyberbezpieczeństwem na

5 N. Neshenko i in., *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*, „IEEE Communications Surveys & Tutorials" 2019, t. 21, nr 3, s. 2702–2733; M. Zhuge Yu i in., *A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices*, „Future Internet" 2020, t. 12, nr 2, nr art. 27.

6 Przeglądy tego typu rozwiązań zob. m.in.: A. Khraisat i in., *Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges*, „Cybersecurity" 2019, t. 2, nr 20, s. 1–22; N. Gupta, P. Chatterjee, T. Choudhury, *Smart and Sustainable Intelligent Systems*, 2021, Wiley Online Library, DOI:10.1002/9781119752134.

poziomie organizacyjnym i technicznym (SOC – Security Operation Center). Jednostki te są wyposażane w zestawy narzędzi i usług pozwalających na monitorowanie sieci w czasie rzeczywistym i budowanie pełnego obrazu sytuacyjnego (SIEM – Security Information and Event Management). Integracja wiedzy z bezpieczeństwa informacji, procesów i technologii służących do monitorowania, analizowania i ochrony organizacji przed cyberatakami pozwala organizacjom szybko reagować na włamania i stale doskonalić procesy wykrywania i zapobiegania atakom. Tym samym systemy IDS/IPS i SIEM odpowiadają za gromadzenie, analizowanie i korelowanie danych. To zintegrowane rozwiązanie bezpieczeństwa, które łączy ciągłe monitorowanie w czasie rzeczywistym i dane z punktów końcowych z opartymi na regułach możliwościami automatycznego reagowania i analizy.

Podsumowując, zdolność do utrzymania bezpieczeństwa sieci i systemów zależy od znajomości krajobrazu zagrożeń, nowych ataków i trendów oraz podatności sprzętu i oprogramowania. Wymaga również specjalistycznych narzędzi do monitorowania globalnej sytuacji, wykrywania zdarzeń związanych z bezpieczeństwem i dostarczania danych operatorom sieci. Zespoły badawczo-rozwojowe prowadzą intensywne prace związane z zastosowaniem nowych metod, mechanizmów i technologii. W ostatnich latach obserwuje się duże zainteresowanie wykorzystaniem technik sztucznej inteligencji. Powstają nowe usługi i innowacyjne produkty umożliwiające wykrywanie i przeciwdziałanie zagrożeniom, które w znaczący sposób zwiększają bezpieczeństwo państwa, w tym ważnych instytucji i obywateli.

Metody sztucznej inteligencji w systemach wykrywania cyberataków

W literaturze dostępnych jest wiele prac prezentujących wyniki badań, których celem jest opracowanie nowych metod i narzędzi do ochrony sieci teleinformatycznych. Można wymienić wiele technik wykrywania złośliwego oprogramowania. Najważniejsze to:

1) analiza wzorców zagrożeń (sygnatur), czyli porównywanie przepływów w sieci oraz zachowań systemów i aplikacji z zestawem wcześniej utworzonych wzorców zagrożeń;

2) wykrywanie anomalii polegające na detekcji nieprawidłowych zachowań, w tym odbiegających od normy, nietypowych obciążeń sieci, specyficznych sekwencji instrukcji w kodzie aplikacji itp.

Metody wykorzystujące sygnatury pozwalają na szybką i skuteczną identyfikację złośliwego oprogramowania, ale mogą być stosowane tylko do wykrywania już znanych ataków. Wzorce są generowane na dwa sposoby, tj. tworzone manualnie lub wyznaczane automatycznie[7]. Generowanie wzorców zagrożeń wymaga eksperckiej wiedzy, jest żmudnym i skomplikowanym procesem. Do detekcji nowych zagrożeń i wykrywania anomalii stosuje się techniki eksploracji wiedzy i danych, odkrywa ukryte relacje, konstruuje różnego rodzaju heurystyki[8].

Tradycyjne podejścia do bezpieczeństwa cybernetycznego zakładające wykorzystanie baz danych o zagrożeniach oraz bazujące na doświadczeniu i wiedzy ekspertów są niewystarczające w przypadku ataków nowej generacji. W ostatnich latach coraz intensywniej do budowania modeli decyzyjnych wykorzystuje się sztuczną inteligencję (artificial intelligence – AI), a w szczególności uczenie maszynowe (machine learning – ML), które na podstawie wyszukiwania relacji w danych uczących pozwala na wydobycie istotnych informacji i wykrycie cyberzagrożenia. Najczęściej stosowanymi modelami obliczeniowymi są sztuczne sieci neuronowe (artificialneural networks – ANN) tworzone przez sztuczne neurony, imitujące w sposób uproszczony działanie ludzkiego mózgu. Obecnie dominują sieci głębokie, składające się z wielu warstw neuronów, z których każda przekształca dane wejściowe w informacje wykorzystywane przez kolejne warstwy. Mówimy wówczas o uczeniu głębokim (deep learning). Artykuł pt. „Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities"[9] zawiera przegląd publikacji z ostatnich lat poświęconych zastosowaniu AI do monitorowania sieci i wykrywania incydentów bezpieczeństwa, w tym nieprawidłowego ruchu i niebezpiecznych zachowań oraz uwierzytelniania użytkowników. Autorzy, omawiając różne podejścia, zwracają uwagę na ograniczenia i istotne wyzwania. Prezentują również autorski, koncepcyjny model cyberbezpieczeństwa. Przegląd platform obliczeniowych, w których stosuje się uczenie maszynowe do ochrony sieci

7 M. Uddin i in., *Signature-based Multi-Layer Distributed Intrusion Detection System Using Mobile Agents*, „International Journal of Network Security" 2013, nr 15, s. 97–105; P. Szynkiewicz, A. Kozakiewicz, *Design and Evaluation of a System for Network Threat Signatures Generation*, „Journal of Computational Science" 2017, t. 22, s. 187–197.

8 W. Wang, W. Wuy, *Online Detection of Network Traffic Anomalies Using Degree Distributions*, „International Journal of Communications, Network and System Sciences" 2010, nr 3, s. 177–182.

9 Z. Zhang i in., *Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities*, „Artificial Intelligence Review" 2022, t. 55, s. 1029–1053.

i systemów komputerowych, zawiera artykuł pt. „A Survey on Representation Learning Efforts in Cybersecurity Domain”[10]. Zastosowanie głębokiego uczenia do detekcji robaków sieciowych jest opisane w artykule pt. „A Worm Detection System Based on Deep Learning”[11].

Uczenie maszynowe jest również coraz częściej wykorzystywane do detekcji ataków na sieci i urządzenia mobilne. Przeglądu wybranych rozwiązań dokonano w artykule pt. „A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks”[12]. W kolejnej sekcji niniejszego artykułu jest omawiany autorski klasyfikator wykorzystujący głębokie uczenie do wykrywania złośliwych aplikacji mobilnych.

Do oceny skuteczności algorytmów detekcji cyberataków bazujących na uczeniu maszynowym wykorzystuje się różne miary. W przypadku klasyfikatora binarnego, który rozróżnia dwie sytuacje, tj. wystąpienie ataku (klasa pozytywna) oraz zachowanie normalne (klasa negatywna), wskaźniki jakości klasyfikacji są liczone na podstawie wartości macierzy błędów (confusion matrix) zawierającej wyniki klasyfikacji. Są to cztery wartości: TP (True Positive) – liczba rzeczywistych ataków zaklasyfikowanych do klasy pozytywnej (poprawnie) i FN (False Negative) zaklasyfikowanych do klasy negatywnej (niepoprawnie) oraz TN (True Negative) – liczba wyników świadczących o normalnym stanie systemu zaklasyfikowanych do klasy negatywnej (poprawnie) i FP (False Positive) zaklasyfikowanych do klasy pozytywnej (niepoprawnie). Poniżej prezentowane są trzy główne miary do oceny jakości klasyfikacji.

1. Dokładność (accuracy) – określa prawdopodobieństwo poprawnej klasyfikacji

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}. \tag{1}$$

2. Precyzja – pokazuje jaka część wyników sklasyfikowanych jako pozytywne należy faktycznie do klasy pozytywnej

$$Precision = \frac{TP}{TP + FP}. \tag{2}$$

10 M. Usman i in., *A Survey on Representation Learning Efforts in Cybersecurity Domain*, „ACM Computing Surveys” 2019, t. 52, s. 1–28.

11 H. Zhou i in., *A Worm Detection System Based on Deep Learning*, „IEEE Access” 2020, t. 8, s. 205444–205454.

12 E. Rodríguez i in., *A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks*, „IEEE Communications Surveys &Tutorials” 2021, t. 23, nr 3, s. 1920–1955.

3. Czułość – określa zdolność klasyfikatora do wykrywania klasy pozytywnej

$$Sensitivity = \frac{TP}{TP + FN}. \quad (3)$$

Przykład zastosowania sztucznych sieci neuronowych do wykrywania złośliwych aplikacji mobilnych

System Android jest obecnie dominującym systemem operacyjnym dla urządzeń mobilnych. Korzysta on z aplikacji, które są zazwyczaj dystrybuowane jako pliki APK (Android Package Kit). Jest to skompresowane archiwum składników danej aplikacji. Podstawowymi elementami APK są: 1) plik AndroidManifest.xml zawierający informacje o aplikacji, w tym charakterystyczne atrybuty, 2) plik classes.dex zawierający m.in. skompilowany kod aplikacji. Decyzja o tym, czy dana aplikacja jest złośliwa jest najczęściej podejmowana na podstawie aktualnej zawartości jednego lub obu wymienionych plików[13].

Zaprojektowany i wykonany autorski system wykrywania złośliwych aplikacji mobilnych na urządzeniach pracujących pod kontrolą systemu Android stosuje analizę statyczną kodu zawartego w pliku classes.dex. Na potrzeby detekcji cyberzagrożeń zbudowano dwa klasyfikatory – dwa modele złożonych sztucznych sieci neuronowych:

1) CNN – splotowa sieć neuronowa;
2) RCNN – rekurencyjna sieć neuronowa z warstwami splotowymi[14].

Do uczenia i testowania sieci wykorzystano 3339 odpowiednio przetworzonych próbek aplikacji szkodliwych pobranych z repozytorium próbek złośliwego oprogramowania VirusShare[15] oraz 3390 próbek aplikacji nieszkodliwych z witryny F-Droid[16]. Podział zbioru był następujący: zbiór uczący – 80% próbek, zbiory walidujący i testowy – po 10% próbek. Obie sieci zostały wytrenowane na zbiorze uczącym. Modele, dla których uzyskano najlepsze wyniki detekcji dla zbioru walidacyjnego, zostały wybrane do eksperymentów

13 S. Arshad, A. Khan, A. Mansoor, M. Shah, *Android Malware Detection and Protection: A Survey*, „International Journal of Advanced Computer Science and Applications" 2016, t. 7, nr 2, s. 342–351; Z. Ren i in., *End-to-End Malware Detection for Android IoT Devices Using Deep Learning*, „Ad Hoc Networks" 2020, t. 101, s. 102098.
14 Ch.C. Aggarwal, *Neural Networks and Deep Learning*, Cham 2018.
15 https://virusshare.com/.
16 https://www.f-droid.org/.

mających na celu sprawdzenie skuteczności klasyfikatorów. Wykonano po kilkanaście eksperymentów dla każdej sieci. Wykorzystano do tego celu zbiór testowy złożony z próbek złośliwych i niezłośliwych. Uśrednione i najlepsze wartości miar zdefiniowanych formułami (1)–(3) prezentuje tabela 1.

Tabela 1. Porównanie skuteczności dwóch modeli klasyfikatorów na przykładzie dziesięciu eksperymentów

Model sieci	Średnie wartości miar [%]			Wartości miar dla modeli o najwyższej uzyskanej dokładności [%]		
	Acc	Precision	Sensitivity	Acc	Precision	Sensitivity
CNN	84,94	88,97	79,70	86,57	88,61	83,83
RCNN	87,96	91,54	83,35	93,28	93,92	92,51

Źródło: R. Litka, *Detekcja złośliwych aplikacji na urządzenia mobilne z wykorzystaniem uczenia maszynowego*, Warszawa 2021.

Wyniki testów potwierdzają wysoką skuteczność opracowanych narzędzi do wykrywania złośliwych aplikacji mobilnych. Pokazują także dość istotną przewagę klasyfikatora, w którym dodano warstwy rekurencyjne. Rozbudowa struktury sieci skutkuje, oczywiście większą złożonością obliczeniową. Czas uczenia sieci RCNN był około cztery razy dłuższy niż sieci CNN. Niemniej jednak ponad 5-procentowe zwiększenie dokładności klasyfikacji danych może istotnie wpłynąć na dokładność wykrywania ataków.

Podsumowanie

Większość powszechnie używanych urządzeń takich jak smartfony, ale również tablety, laptopy itp. pracuje pod kontrolą systemu Android. Stąd ważne jest zapewnienie bezpieczeństwa i ochrona przed cyberatakami tego systemu oraz aplikacji działających pod jego kontrolą. Prezentowany przykład zastosowania dwóch modeli klasyfikatorów wykorzystujących głębokie uczenie do wykrywania złośliwych aplikacji na urządzenia mobilne potwierdza, że narzędzia informatyczne wykorzystujące metody sztucznej inteligencji mogą znacząco wspierać zespoły zajmujące się cyberbezpieczeństwem. Należy podkreślić, że opracowane i wykonane klasyfikatory mogą pracować w pełni autonomicznie, a przeprowadzone dodatkowe eksperymenty potwierdzają, że ich skuteczność rośnie wraz ze wzrostem wolumenu danych uczących. Koszt obliczeniowy nie jest duży, uczenie przebiega szybko, więc może być realizowane na urządzeniu o niewielkich zasobach, jakim jest np. telefon komórkowy.

Bibliografia

Aggarwal Ch.C., *Neural Networks and Deep Learning*, Cham 2018.

Arshad S., Khan A., Mansoor A., Shah M., *Android Malware Detection and Protection: A Survey*, „International Journal of Advanced Computer Science and Applications" 2016, t. 7, nr 2.

Gupta N., Chatterjee P., Choudhury T., *Smart and Sustainable Intelligent Systems*, 2021, Scrivener Publishing LLC, Wiley Online Library.

Khraisat A. i in., *Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges*, „Cybersecurity" 2019, t. 2, nr 20.

Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2021, Warszawa 2022.

Litka R., *Detekcja złośliwych aplikacji na urządzenia mobilne z wykorzystaniem uczenia maszynowego*, Warszawa 2021.

Mobile security report 2021, Izrael 2022.

Neshenko N. i in., *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*, „IEEE Communications Surveys & Tutorials" 2019, t. 21, nr 3.

Ren Z. i in., *End-to-End Malware Detection for Android IoT Devices Using Deep Learning*, „Ad Hoc Networks" 2020, t. 101.

Rodríguez E. i in., *A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks*, „IEEE Communications Surveys & Tutorials" 2021, t. 23, nr 3.

Shishkova T., Kivva A., *Mobile malware evolution 2021*, 21 Feb 2022, https://securelist.com/mobile-malware-evolution-2021/105876/ [dostęp: 10.01.2023].

Szynkiewicz P., Kozakiewicz A., *Design and Evaluation of a System for Network Threat Signatures Generation*, „Journal of Computational Science" 2017, t. 22.

Uddin M. i in., *Signature-based Multi-Layer Distributed Intrusion Detection System Using Mobile Agents*, „International Journal of Network Security" 2013, nr 15, s. 97–105.

Usman M. i in., *A Survey on Representation Learning Efforts in Cybersecurity Domain*, „ACM Computing Surveys" 2019, t. 52.

Wang W., Wuy W., *Online Detection of Network Traffic Anomalies Using Degree Distributions*, „International Journal of Communications, Network and System Sciences" 2010, nr 3, s. 177–182.

Zhang Z. i in., *Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities*, „Artificial Intelligence Review" 2022, t. 55.

Zhou H. i in., *A Worm Detection System Based on Deep Learning*, „IEEE Access" 2020, t. 8.

Zhuge Yu M. i in., *A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices*, „Future Internet" 2020, t. *12*, *nr 2*.

Attacks on mobile devices and methods of detection

Abstract

Individual protection of autonomous systems using simple analysis of transmitted messages is unfortunately becoming insufficient. There is a clear need for new solutions using data from multiple sources, integrating various methods, mechanisms and algorithms, including Big Data processing and data classification techniques using artificial intelligence methods. The quantity, quality, reliability and timeliness of data and information about the network situation, as well as the speed of its processing, determine the effectiveness of protection. The paper presents examples of the application of various artificial intelligence techniques for detecting attacks on ICT systems. Attention is focused on the application of deep learning methods for the detection of malicious

applications installed on mobile devices. The effectiveness of the presented solutions was confirmed by numerous simulation experiments conducted on real data. Promising results were obtained.

Key words: cybersecurity, cyberattack detection, mobile applications, artificial intelligence, machine learning, artificial neural networks, deep learning