Autoreferat

dr inż. Grzegorz Blinowski

POLITECHNIKA WARSZAWSKA

WYDZIAŁ ELEKTRONIKI I TECHNIK INFORMACYJNYCH

Ul. Nowowiejska15/19, 00-660 Warszawa

grzegorz.blinowski@pw.edu.pl

Warszawa, 2024

1. Imię i nazwisko.

Grzegorz Blinowski

2. Posiadane dyplomy, stopnie naukowe lub artystyczne – z podaniem podmiotu nadającego stopień, roku ich uzyskania oraz tytułu rozprawy doktorskiej.

2001	Doktor nauk technicznych w dyscyplinie informatyka, Politechnika Warszawska. Informacje o rozprawie: *Model komunikacji i synchronizacji dla rozproszonych systemów komputerowych*, Wydział Elektroniki i Technik Informacyjnych, Data obrony: 10-07-2001, Data nadania stopnia: 25-09-2001
1993	mgr inż. informatyki Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych.

3. Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych.

2001 – obecnie	Adiunkt, Zakład Oprogramowania i Architektury Komputerów, Instytut Informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska
1993 – 2001	Asystent, Instytut Informatyki, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska

4. Omówienie osiągnięć, o których mowa w art. 219 ust. 1 pkt. 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478 z późn. zm.).

Jako osiągnięcie, o którym mowa w art. 219 ust. 1 pkt. 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce wskazuję cykl powiązanych tematycznie artykułów naukowych, pod zbiorczym tytułem:

„Bezpieczeństwo systemów Internetu Rzeczy (IoT)"

4.1 Wykaz wybranych publikacji

[**A1**] Blinowski, G.: *Security issues in visible light communication systems*, IFAC-PapersOnLine, Vol. 48, No. 4, pp. 234 – 239, Elsevier. 2015.
http://dx.doi.org/10.1016/j.ifacol.2015.07.039
Impact Factor: 0.30; Punkty MNiSW: 20

[**A2**] Blinowski, G., *Practical aspects of physical and MAC layer security in visible light communication systems*, International Journal of Electronics and Telecommunications, Vol. 62, No. 1, pp. 7 – 13. 2016.
http://dx.doi.org/10.1515/eletel-2016-0001
Impact Factor: 0.7; Punkty MNiSW: 70

[**A3**] Blinowski, G., Kmieciak, A., *Modelling and evaluation of a multi-tag LED-ID platform*, Proc. Federated Conference on Computer Science and Information Systems (FEDCSIS), Gdańsk, Poland, 11 - 14 September. 2016.

Mój wkład w powstanie tej pracy polegał na opracowaniu koncepcji badania, udziale w przygotowaniu i prowadzeniu symulacji oraz pomiarów, a także na opracowaniu wyników i napisaniu artykułu. Mój udział procentowy wynosi 80%.

[**A4**] Blinowski, G.; Szczypiorski, K., *Steganography in VLC Systems*, Journal of Universal Computer Science, Vol. 23, No. 5, pp. 454-478. 2017. http://dx.doi.org/10.3217/jucs-023-05-0454
Impact Factor: 1.066; Punkty MNiSW: 40

Mój wkład w powstanie tej pracy polegał na opracowaniu założeń i rozwiązań steganograficznych dla VLC, a także w znacznej mierze na napisaniu artykułu. Mój udział procentowy wynosi 75%.

[**A5**] Blinowski, G., *The feasibility of launching rogue transmitter attacks in indoor visible light communication networks*, Wireless Personal Communications, Vol 97, pp. 5325-5343,2017, Springer US. 2017. http://dx.doi.org/10.1007/s11277-017-4781-3
Impact Factor: 2.2; Punkty MNiSW: 40

[**A6**] Blinowski, G., Januszewski, P., Stepniak, G., Szczypiorski, K., *LuxSteg*: *First practical implementation of steganography in VLC*, IEEE Access,Vol. 6, pp. 74366-74375, IEEE. 2018. http://dx.doi.org/10.1109/ACCESS.2018.2883250
Impact Factor: 4.098; Punkty MNiSW: 100

Mój wkład w powstanie tej pracy polegał na współuczestniczeniu w opracowaniu koncepcji badania oraz opracowaniu wyników i napisaniu artykułu. Mój udział procentowy wynosi 40%.

[**A7**] Blinowski, G., *Security of visible light communication systems—A survey*, Physical Communication, Vol. 34, pp. 246-260, Elsevier. 2019.
http://dx.doi.org/10.1016/j.phycom.2019.04.003
Impact Factor: 2.2; Punkty MNiSW: 70

[**A8**] Blinowski, G., Mościcki, A., *Comparing Gausian and exact models of malicious interference in VLC systems*, International Journal of Electronics and Telecommunications, Vol. 65. 2019. http://dx.doi.org/10.24425/ijet.2019.126311
Impact Factor: 0.7; Punkty MNiSW: 70

Mój wkład w powstanie tej pracy polegał na opracowaniu koncepcji badania, udziale w przygotowaniu i prowadzeniu symulacji, a także na opracowaniu wyników i napisaniu artykułu. Mój udział procentowy wynosi 75%.

[**A9**] Blinowski, G., *Risk-Based Decision Making in IoT Systems*, Information Systems Architecture and Technology: Proceedings of 38th International Conference on

Information Systems Architecture and Technology – ISAT 2017. Part I / Borzemski Leszek, Świątek Jerzy, Wilimowska Zofia (*red.*), Advances in Intelligent Systems and Computing, vol. 655, Cham, Springer, s.230-241, ISBN 978-3-319-67219-9. 2018. http://dx.doi.org/10.1007/978-3-319-67220-5_21
Punkty MNiSW: 20

[**A10**] Blinowski, G., Piotrowski, P., *CVE based classification of vulnerable IoT systems*; International Conference on Dependability and Complex Systems; pp. 82-93, Springer. 2020. DOI: https://doi.org/10.1007/978-3-030-48256-5_9
Punkty MNiSW: 40

Mój wkład w powstanie tej pracy polegał na opracowaniu koncepcji badania, udziale w przygotowaniu i prowadzeniu symulacji i pomiarów, a także na opracowaniu wyników i napisaniu artykułu. Mój udział procentowy wynosi 80%.

[**A11**] Blinowski, G. J., Piotrowski, P., Wiśniewski, M., *Comparing Support Vector Machine and Neural Network Classifiers of CVE Vulnerabilities*, Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021), pages 734-740, ISBN: 978-989-758-524-1. 2021.
http://dx.doi.org/10.5220/0010574807340740
Punkty MNiSW: 70

Mój wkład w powstanie tej pracy polegał na opracowaniu koncepcji badania, udziale w przygotowaniu i prowadzeniu symulacji i pomiarów, a także na opracowaniu wyników i napisaniu artykułu. Mój udział procentowy wynosi 70%.

4.2 Wstęp

Przedstawione osiągnięcie naukowe dotyczy tematyki bezpieczeństwa systemów informatycznych, a dokładnie: bezpieczeństwa systemów Internetu Rzeczy (Internet of Things, IoT) i jest podsumowaniem moich prac prowadzonych od 2013 do 2023 roku. W tym czasie prowadziłem badania naukowe w dwóch głównych nurtach dotyczących:

- szeroko pojętego bezpieczeństwa systemów Visible Light Communication (VLC), tj. wykorzystujących światło widzialne jako nośnik danych;

- analizy ryzyka oraz analizy i klasyfikacji podatności systemów IoT systemów IoT;

Urządzenia Internetu Rzeczy stanowią obecnie większość systemów podłączonych bezpośrednio lub pośrednio do globalnej sieci. Na przełomie pierwszej i drugiej dekady XXI wieku ich liczba przekroczyła dziesięć miliardów, do końca obecnej dekady ma osiągnąć[1] trzydzieści miliardów sztuk [1]. Tak więc liczba systemów IoT przekracza kilkakrotnie liczbę systemów mających bezpośredni kontakt z użytkownikami (tj. smartfonów i innych podobnych urządzeń mobilnych, komputerów przenośnych oraz stacjonarnych). Technologie systemów IoT w ostatniej dekadzie rozwijały się niezwykle dynamicznie, przede wszystkim w zakresie sensorów i układów wykonawczych, ale także w obszarze protokołów i algorytmów komunikacji. Tak jak miało to miejsce z innymi technologiami w przeszłości (np. w przypadku rozwoju sieci internetowych), przy opracowywaniu nowych, nierzadko pionierskich rozwiązań, kwestie szeroko rozumianego bezpieczeństwa często schodziły na drugi plan lub były niemal całkowicie pomijane. Taka praktyka, wynikająca z chęci szybkiego dostarczenia i wdrożenia nowych technologii, skutkowała poważnymi konsekwencjami związanymi z naruszeniem bezpieczeństwa danych i systemów. Prowadzone przeze mnie prace skupiały się na identyfikacji, opisaniu oraz eliminacji zagrożeń w zakresie nowych technologii IoT i tym samym na wypełnieniu luki związanej z niewystarczajacym zaadresowaniem kwestii bezpieczeństwa w systemach IoT.

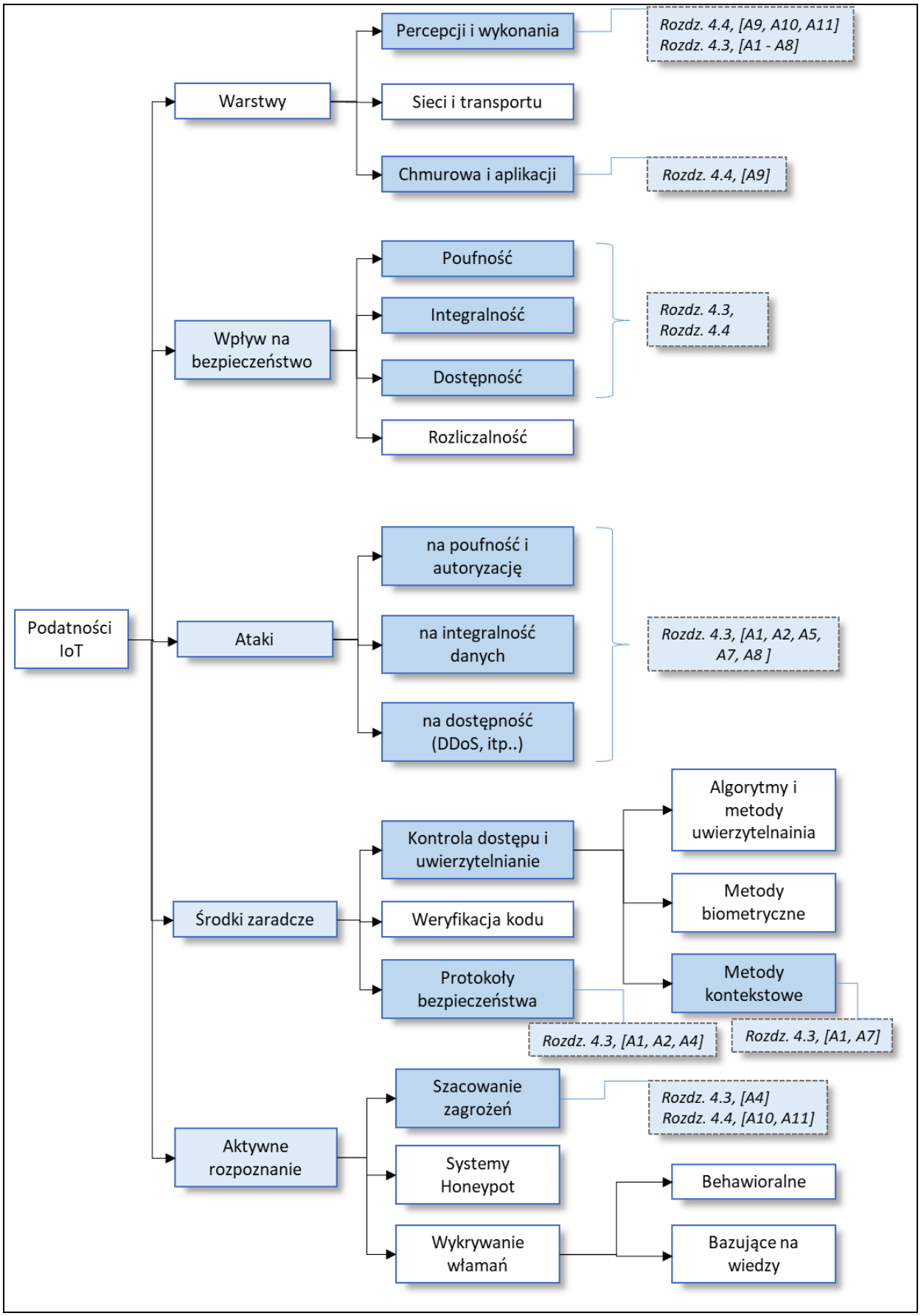
Kwestie bezpieczeństwa systemów IoT nabierają więc pierwszorzędnego znaczenia zarówno dla użytkowników końcowych, jak i operatorów i dostawców usług, przedsiębiorstw i wszelkich organizacji korzystających z usług elektronicznych. Aspekt ten jest też szczególnie istotny z uwagi na branże, w których technologie IoT w ostatniej dekadzie szczególnie się rozwinęły [2], tj. w: ochronie zdrowia, zarządzaniu łańcuchami dostaw, usługach komunalnych i monitorowaniu oraz ochronie środowiska. Masowa skala wdrożeń konsumenckich rozwiązań IoT powoduje, że wadliwe zabezpieczenia (lub nawet ich brak) skutkują wielkoskalowymi atakami na światową infrastrukturę internetową. Przykładem takich zdarzeń były ataki prowadzone przez botnety takie jak: Qbot, Carna, VPNFilter, Mirai [3], obejmujące setki tysięcy przejętych urządzeń.

Ogólnie pojęta problematyka cyber-bezpieczeństwa, obejmuje między innymi zapewnienie: poufności, integralności, autentyczności, dostępności danych w ruchu i spoczynku. Z kolei tematyka bezpieczeństwa systemów IoT dotyczy ujęcia tych kwestii w szeregu bardzo różnorodnych platform sprzętowych (od prostych jednofunkcyjnych systemów wbudowanych po serwery chmurowe), także w kontekście różnych protokołów LAN, WLAN i WAN oraz dla

[1] Według innych oszacowań będzie to nawet 500 miliardów sztuk. Różnice te wynikają z metod klasyfikacji prostych jednofunkcyjnych sensorów i układów wykonawczych.

wielkiej liczby różnorodnych aplikacji. Badania prowadzone w tak szerokim obszarze jakim jest IoT, siłą rzeczy, dotyczyć mogą stosunkowo wąskich wybranych dziedzin, technologii i aplikacji. Dominującą w literaturze przeglądowej (np. w [2, 4]) metodyką klasyfikacji aspektów bezpieczeństwa jest wyjście od potencjalnych podatności systemów IoT, a następnie zaadresowanie: ataków, ich skutków, środków zaradczych, itd. związanych z tymi podatnościami. Na rysunku 1 przedstawiono klasyfikację bazującą na [2]. Kolorami oznaczono obszary, które stanowiły zakres moich badań opisanych w niniejszym autoreferacie. W odnośnikach wykonanych jasniejszym kolorem podano rozdział niniejszego autoreferatu oraz pozycje z bibliografii (rozdz. 4.1), w których poruszono dane zagadnienie.

W niniejszych autoreferacie zaprezentowane zostaną główne osiągnięcia naukowe autora, które wybrane zostały jako jego istotny wkład w zwiększenie poziomu bezpieczeństwa systemów IoT. Główna część autoreferatu podzielona została na dwa podrozdziały odpowiadające dwóm grupom zagadnień, będących przedmiotem jego najważniejszych publikacji naukowych autora. Są to odpowiednio: (1) nowe, kompleksowe rozwiązania problemów bezpieczeństwa systemów VLC; (2) oryginalne rozwiązania z zakresu analizy ryzyka i klasyfikacja podatności w złożonych systemach IoT.



Rysunek 1 *– Klasyfikacja obszarów bezpieczeństwa IoT z zaznaczonymi obszarami ujętymi w niniejszym autoreferacie (bazująca na [2])*

4.3 Analiza bezpieczeństwo VLC

Charakterystyka VLC i jego bezpieczeństwa

Określenie „Visible Light Communication" nie oddaje precyzyjnie charakteru technologii VLC i wymaga wyjaśnienia. Systemy VLC realizują transmisję danych z wykorzystaniem światła widzialnego (zakres długości fal od 780 do 375 nm) bez korzystania ze światłowodów lub innego fizycznego medium transmisji i na niewielkie odległości – od dziesiątków centymetrów do kilku (rzadziej kilkunastu) metrów. VLC jest więc podzbiorem Optical Wireless Communication (OWC), która wykorzystuje także zakresy podczerwieni oraz ultrafioletu, nie powinna być też mylona z Free Space Optical Communication (FSOC), które to miano zwyczajowo zarezerwowano dla silnie kierunkowej transmisji realizowanej przy pomocy nadajników laserowych.

Systemy VLC swoje powstanie i rozwój zawdzięczają popularyzacji tanich i energooszczędnych systemów oświetlenia, bazujących na półprzewodnikowych źródłach światła LED [5]. Istotą idei VLC jest wykorzystanie standardowych źródeł światła w roli nadajników w transmisji danych, co realizowane jest poprzez odpowiednią modulację o częstościach nie dostrzegalnych dla ludzkiego oka (a więc nie powodujących uczucia dyskomfortu). VLC może wykorzystywać takie źródła światła jak: standardowe oświetlenie pomieszczeń (panele, źródła punktowe), światła uliczne, światła pojazdów (pojazdy naziemne kołowe, pojazdy podwodne), oświetlenie lub „doświetlenie" witryn sklepowych, jak i źródła przenośne lub pół-przenośnie: smartfony i inne podobne urządzenia, lampy biurkowe, itp.

Poważny wzrost zainteresowania tym sposobem komunikacji nastąpił w pierwszej dekadzie XXI wieku dzięki pilotowym wdrożeniom realizowanym na rynku japońskim [6] oraz dzięki projektowi „Omega" realizowanemu w Unii Europejskiej [7]. W roku 2011 zatwierdzono pierwszą wersję standardu dotyczącego VLC tj. IEEE 802.15.7 [8].

Dość częstym zjawiskiem obserwowanym w pierwszej fazie rozwoju nowych technik komunikacji cyfrowej jest zaniedbywanie kwestii bezpieczeństwa. W przypadku VLC temat ten adresowany był przy pomocy sloganu WYSIWYS „*What You See Is What You Send*" (widzisz to co wysyłasz), oznaczającego, że w środowisku, w którym nadajnik i odbiornik pozostają we wzajemnej fizycznej relacji „bezpośredniej widoczności" kwestie bezpieczeństwa mają drugorzędne znaczenie, gdyż każdy intruz lub strona podsłuchująca zostaną łatwo fizycznie zlokalizowani [9]. Jako potwierdzenie nieadekwatności określenia „WYSIWYS" do aspektów bezpieczeństwa, można przytoczyć fakt, iż w ww. standardzie

IEEE 802.15.7 jedynym odniesieniem do szeroko pojętych kwestii bezpieczeństwa jest wprowadzenie opcjonalnego szyfrowania transmisji kluczem symetrycznym, bez odniesienia się np. do kwestii wymiany kluczy.

W pracach [A1, A2] przedstawiłem[2] po raz pierwszy w literaturze systematyczny przegląd kwestii bezpieczeństwa VLC ujętych w ramy jakościowej analizy ryzyka dla zdarzeń takich jak: zakłócanie, podsłuchiwanie i modyfikacja przesyłanych danych w różnych fizycznych scenariuszach. Scenariusze te objęły komunikację pomiędzy stronami takimi jak: urządzenia mobilne (telefony, tablety), urządzenia stacjonarne (komputery desktop, inne urządzenia komputerowe) oraz stałe elementy infrastruktury (typowo jest to oświetlenie pomieszczeń realizujące jednocześnie funkcje transmisji danych). Odniosłem się do sześciu potencjalnych trybów komunikacji wynikających z rodzaju nadajnika i odbiornika (kierunkowy / dyfuzyjny) oraz sposobu komunikacji (bezpośrednia widoczność nadajnika i odbiornika lub jej brak). Argumentowałem, iż wzajemna widoczność nadajnika i odbiornika nie gwarantuje niemożności ingerencji w transmisję danych. Analiza ryzyka wykazała istnienie największych potencjalnych zagrożeń dla komunikacji z systemami infrastruktury. Na podstawie Poissonowskiego modelu kanału pokazałem, że transmisja VLC może był zakłócona zarówno przez pojedyncze źródło o mocy porównywalnej z mocą legalnego nadajnika, jak i przez wiele źródeł o niższej mocy. Poissonowski kanał VLC może zostać całkowicie wysycony przez wrogie nadajniki. W pracy przeanalizowałem też i odniosłem się do mechanizmów bezpieczeństwa zdefiniowanych w standardzie IEEE 802.15.7, tj. w szczególności: dopuszczenia trybu „None", pozwalającego na brak szyfrowania i kontroli integralności oraz trybów „encryption-only" i „integrity-only" oraz braku procedur uzgadniania kluczy. Wskazałem, że VLC bazujące na tym standardzie oprócz oczywistych niedostatków narażone jest na ataki związane z brakiem szyfrowania niektórych pól nagłówka MAC, zaś zastosowanie kluczy grupowych naraża system na ataki od wewnątrz tj. z obrębu grupy.

Należy zaznaczyć, że wcześniej ukazały się pojedyncze prace dotyczące przechwytywania transmisji oraz jej bezpieczeństwa w kontekście teorii informacji [10], żaden z autorów nie analizował jednak systemów VLC kompleksowo, tj. w ujęciu różnych konfiguracji sprzętowych i wszystkich potencjalnych zagrożeń. Kwestie to zeostały po raz pierwszy wszechstronnie i wyczerpująco podjęte w wyżej wymienionych pracach habilitanta.

[2] Praca [A2] stanowi rozszerzoną wersję konferencyjnego artykułu [A1].

Prace [A1, A2] uzyskały łącznie (wg. Google Scholar) 84 cytowania. Analiza wybranych referencji, ograniczonych do prac, które ukazały się w "punktowanych" czasopismach oraz konferencjach wykazała:

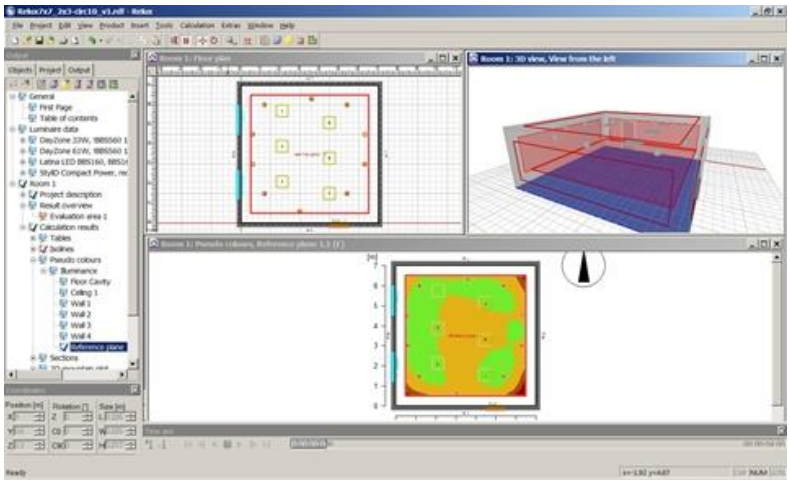
- Prac przeglądowych ("Survey lub "Review"): 10
- Prac opisujących oryginalne: rozwiązanie, technologię, protokół lub system: 30
- Prac z dziedziny bezpieczeństwa VLC: 12
- Prac z dziedziny ustalania i dystrybucji kluczy: 3
- Prac opisujących nowy system lub rozwiązanie VLC: 12
- Prac z zakresu analizy ryzyka: 2
- Prac przeglądowych o zakresie szerszym niż VLC: 3
- Prac z zakresu rozwiązań VANET: 4

Autorzy wymienionych prac najczęściej powołują się na: przedstawioną w [A1, A2] metodykę analizy ryzyka w VLC; analizę protokołów IEEE 802.15.7 oraz kwestie dotyczące wrogiego zakłócania i podsłuchu. Wyżej wymienione artykuły ukazały się m.in. w: ACM Computing Surveys, Electronics, IEEE Access, IEEE Communications Surveys, IEEE Photonics Technology Letters, IEEE/ACM Transactions on Networking, International Symposium on Networks, Computers and Communications (ISNCC), Physical Communication, Plos One, Sensors, Signal Processing, Vehicular Communications i były cytowane łącznie 654 razy (stan na kwiecień 2024).

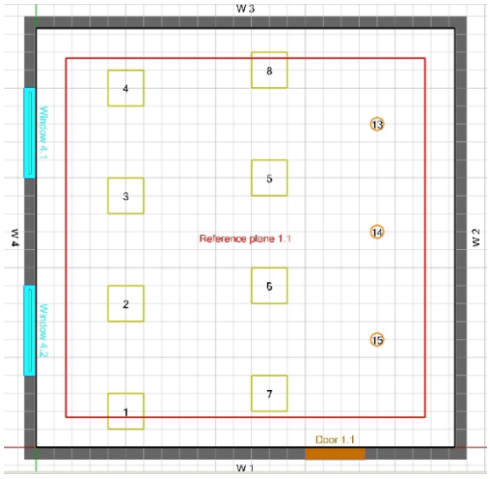
Modelowanie i symulacje wrogich transmisji VLC

Logiczną konsekwencją wyżej opisanych ustaleń było przedstawienie praktycznych realizacji systemów VLC, w których mogłoby dochodzić do naruszeń bezpieczeństwa polegających na zakłócaniu i/lub modyfikacji transmisji. W pracy [A5] przedstawiłem wyniki badań symulacyjnych, obejmujących kilkanaście scenariuszy komunikacji z udziałem infrastruktury VLC w przestrzeni „biurowej”, w której zainstalowano jeden lub więcej wrogich nadajników. Poprzednie prace, których symulacyjnie badano różne aspekty funkcjonowania VLC bazowały na bardzo uproszczonym modelu środowiska (ustandaryzowane pomieszczenie o niewielkich rozmiarach (rzędu 4 m x 4 m), cztery źródła światła) [10]. Modele, które przedstawiłem w [A5] odpowiadały realnym, a nie wyidealizowanym środowiskom fizycznym (tak jak miało to miejsce we wcześniejszych przytaczanych pracach innych autorów). Dlatego też, punktem wyjścia do realizacji symulacji było stworzenie, za pomocą specjalizowanego programu CAD, projektu biurowej przestrzeni użytkowej typu „open space”, w której oświetlenie LED spełnia wymagania

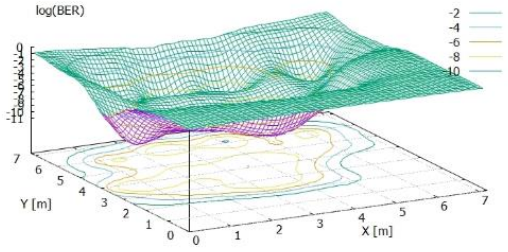
stawiane odpowiednim normom budowlanym i ergonomicznym, i jednocześnie wykorzystuje dostępne komercyjnie panele lub punktowe źródła LED. Tak utworzony model (rysunek 2) stał się punktem wyjścia do symulacji, których celem było obliczenie stopy błędów transmisji (Bit Error Rate – BER), dla różnej liczby, typu i rozmieszczeń wrogich nadajników w ogólnej konfiguracji wielu źródeł i jednego odbiornika (Multiple Input Single Output – MISO). Model matematyczny (bazujący na pionierskich pracach [11]) użyty do symulacji uwzględniał takie parametry fizyczne, jak między innymi: fizyczna charakterystyka źródła światła (rozmiary, liczba LED, moc, półkąt oświetlenia), geometria pomieszczenia i parametry odbiornika. Program symulacyjny obliczał addytywnie moc świetlną w danym punkcie, z uwzględnieniem odbić pierwszego rzędu. Na tej podstawie wyznaczano stosunek sygnału do szumu (z uwzględnieniem szumów termicznego, odbiornika oraz ISI), zaś z tej wielkości bezpośrednio (przy założeniu konkretnej modulacji) obliczyć można BER.



(A)



(B)



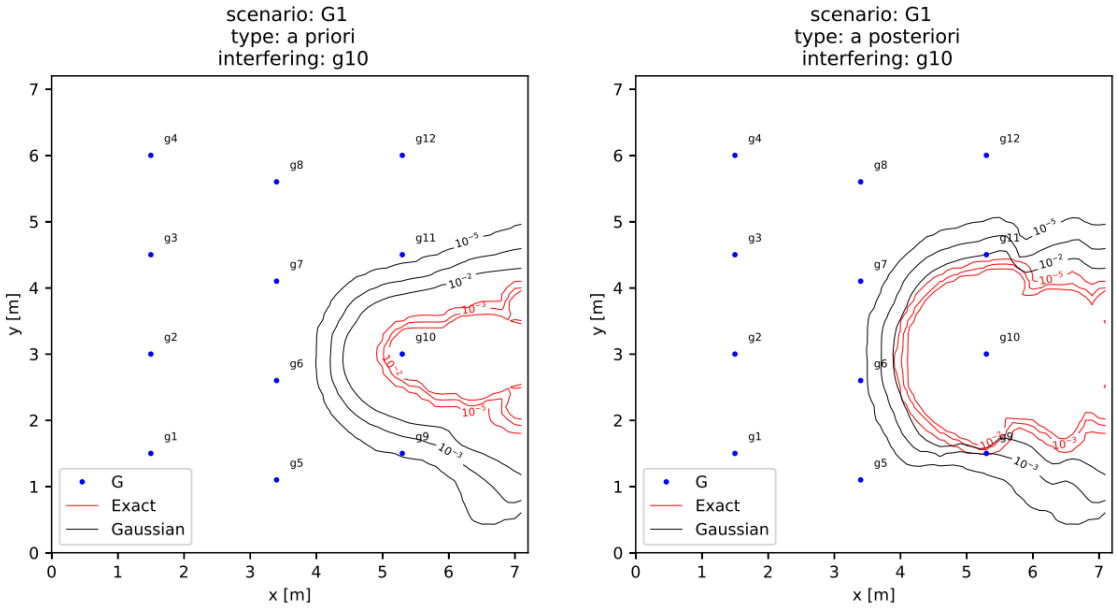
(C)

Rysunek 2 *– A - projekt symulowanego obszaru; B - schemat rozmieszczenia źródeł światła; C - obliczona numerycznie wartość BER dla powierzchni referencyjnej.*

Łącznie zbadałem trzy konfiguracje rozmieszczenia źródeł światła, z odpowiednio: jednym, dwoma i trzema różnymi wrogimi nadajnikami – w sumie czternaście oddzielnych konfiguracji, które poddano symulacji. Efektem badań symulacyjnych było potwierdzenie, że nawet jeden wrogi nadajnik niskiej mocy może zakłócać odbiór danych pochodzących z legalnych źródeł na 75% badanego obszaru i jednocześnie przejmować transmisję dla 10% badanego obszaru.

Symulacje VLC – metoda przybliżona i dokładna

W metodyce numerycznej symulacji opisanych w [A5] przyjęto jedno dość istotne uproszczenie – założono idealną, tj. Gaussowską i w konsekwencji, addytywną naturę szumu i zakłóceń (czyli wrogiej transmisji). Założenie to jest powszechnie przyjmowane w pracach bazujących na podobnych modelach [11], gdyż znacząco upraszcza obliczenia. Powstaje jednak pytanie – jakie rezultaty osiągnięto by dla modelu „dokładnego", tj. niegaussowskiego? Odpowiedź na to pytanie znajduje się w pracy [A8], której współautorem jest magister inżynier Adam Mościcki realizujący pracownię dyplomową pod moją opieką. Praca wychodzi ze środowiska symulacyjnego opisanego wyżej, w modelu matematycznym uwzględniono jednak dokładną, a nie przybliżoną charakterystykę zakłóceń pochodzących od wrogich nadajników. Przyjęcie tego założenia wymagało istotnego rozbudowania modelu kanału transmisyjnego po stronie odbiorcy, gdyż należało uwzględnić dwa przypadki: nadajników kooperujących oraz niekooperujących (wrogich). Uzyskane symulacyjnie wyniki rozkładu BER okazały się bardzo interesujące: różnice pomiędzy dwoma modelami występują, lecz są stosunkowo niewielkie. Przykładowo: w najbardziej zróżnicowanym przypadku obszar, w którym BER wyniósł 10^{-3} pokrywał 16% pola symulacji dla modelu dokładnego i 30% dla modelu przybliżonego. We wszystkich przeprowadzonych symulacjach różnice w powierzchni tego obszaru wynosiły od 10% do 50%.



Rysunek 3 *– Symulacje przeprowadzone dla jednego zakłucającego nadajnika VLC (w punkcie g10). Kolorem czerwonym i czarnym zaznaczono odpowiednio izolinie BER dla modelu dokładnego i Gaussowskiego. Przypadki a priori oraz a posteriori dotyczą odpowiednio sytuacji w której pozostale nadajniki „wiedzą" lub nie o istnieniu wrogiego nadajnika.*

Przykład jednej z symulacji pokazano na Rysunku 3 - izolinie czerowne obejmujące mniejszy obszar obejmują mniejszą powierzchnię niż izolinie dla modelu przyblizonego (rysunek za praca [A10]). Dla wszystkich objętych symulacją przypadków model dokładny pokazywał mniejszy obszar potencjalnie zagrożony. Istotnym wynikiem pracy jest zatem konstatacja, że symulacje z użyciem modelu przybliżonego dają wynik bardziej pesymistyczny, co w przypadku analizy bezpieczeństwa należy uznać za pozytyw. W tym miejscu należy zaznaczyć, że symulacje z wykorzystaniem modelu dokładnego są znacznie kosztowniejsze obliczeniowo niż z użyciem modelu przybliżonego (dla opisanych wyżej scenariuszy: kilkanaście minut dla jednego scenariusza w modelu dokładnym w stosunku do kilku sekund w modelu przybliżonym na typowym sprzęcie klasy desktop z siatką o rozdzielczości 0,2 m). W pracy tej wykazano zatem po raz pierwszy, że rzeczywiście – przyjmowane do tej pory milcząco i bez należytego uzasadnienia założenie, że model Gaussowski w większości przypadków symulacyjnych jest wystarczający można uznać za zasadne.

Wrogie nadajniki LED-ID – weryfikacja eksperymentalna

Model i metody symulacji przedstawione w pracach [A1, A2, A5] opisane wyżej zweryfikowałem także eksperymentalnie w środowisku sprzętowym LED-ID [12]. Technologia LED-ID (albo LED-TAG) jest świetlnym odpowiednikiem rozwiązań RFID. Stosowana jest np. w muzeach (do identyfikowania eksponatów), a także w handlu detalicznym (do identyfikowania towarów znajdujących się na półkach). Rolę odbiornika w tych zastosowaniach pełni typowo smartfon. Podstawowa różnica pomiędzy infrastrukturalnymi systemami VLC, a systemami LED-ID leży w mocy nadajników, a w konsekwencji w zasięgu komunikacji. Dla LED-ID efektywny zasięg wynosi 20 – 40 cm, jest więc o rząd większości mniejszy niż w przypadku zastosowania VLC do realizacji komunikacji w pomieszczeniach. W pracy [A3], której współautorką była magister inżynier Adriana Kmieciak, realizująca pracownię dyplomową pod moją opieką, zweryfikowano przy pomocy symulacji kilka scenariuszy rozmieszczenia nadajników LED identyfikujących dany obiekt oraz wrogiego nadajnika wnoszącego zakłócenia. Podobnie jak w przypadku infrastrukturalnego VLC stwierdzono, że w różnych fizycznych konfiguracjach możliwe jest wprowadzenie do środowiska wrogiego nadajnika, który będzie miał istotny (negatywny) wpływ na całe środowisko. Wyniki symulacji zostały potwierdzone przy pomocy eksperymentu, w którym wykorzystano sprzęt firmy OLEDCOM – tj. nadajniki zrealizowane w postaci punktowych źródeł światła o półkącie

15º i natężeniu światła ok. 900 lx w odległości 50 cm od źródła. Zestawy OLEDCOM zawierają także odbiorniki podłączane do portu audio smartfona oraz bibliotekę oprogramowania dla systemu Android, przy pomocy której stworzono aplikację pomiarową przesyłającą wyniki do zdalnego serwera (co usprawniło proces zbierania danych). Przeprowadzono eksperymenty w różnych, zmiennych, warunkach środowiskowych, tj. w pomieszczeniu zamkniętym bardzo słabo oświetlonym, oświetlonym rozproszonym światłem LED oraz oświetlonym bezpośrednim światłem słonecznym (od 10 lux do 5000 lux w polu pomiaru). Dla każdych warunków ustalono efektywny zasięg transmisji, a następnie przeprowadzono pomiary z nadajnikiem zakłócającym (wrogim). Wyniki eksperymentu były zgodne, zarówno jakościowo, jak i ilościowo, ze scenariuszem symulacyjnym i potwierdzały skuteczność wrogiego nadajnika. Praca stanowi rozwinięcie modelu teoretycznego i metod symulacyjnych przedstawionych wyżej w [A2, A5] i jest jednocześnie jedną z nielicznych obecnych w literaturze prac podnoszących kwestie bezpieczeństwa systemów LED-ID, dlatego ma w mojej ocenie istotne znaczenie praktyczne.

Praca [A5][3] była cytowana (wg. Google Scholar) w 15 "punktowanych" czasopismach oraz konferencjach. Referencje odnosiły się do zagadnień zakłócania i podsłuchiwania transmisji oraz technik ich unikania i ukazały się m.in. w: ACM Computing Surveys, IEEE Access, IEEE Internet of Things Journal, IEEE International Conference on Communications IEEE Transactions on Wireless Communications, IEEE Photonics Journal, Optics Express oraz Physical Communication. Warto też nadmienić, że praca [A5] cytowana jest w patencie [14] przyznanym przez Biuro Patentów USA, nr patentu: US 11,317,423 B2 zatytułowanym: "*Method and system for managing interference caused by rogue user equipment Li-Fi Communication Network*", patent ten odwołuje się bezpośrednio do wyników przedstawionych w [A5].

Steganografia w VLC

Jedną z istotnych dziedzin bezpieczeństwa transmisji danych jest steganografia. Steganografię [gr. *Steganós* ‘przykryty’, graphe ‘pismo’] definiuje się jako: „*zespół metod służących do bezpiecznego przesyłania informacji w sposób ukrywający sam fakt ich istnienia*” (wg. Encyklopedii PWN). Steganografia ma zastosowanie zarówno do danych pozostających w spoczynku – np. ukrywanie informacji w plikach obrazów lub audio, jak i

[3] Łącznie z wersją dostępną w serwisie ArXiv.

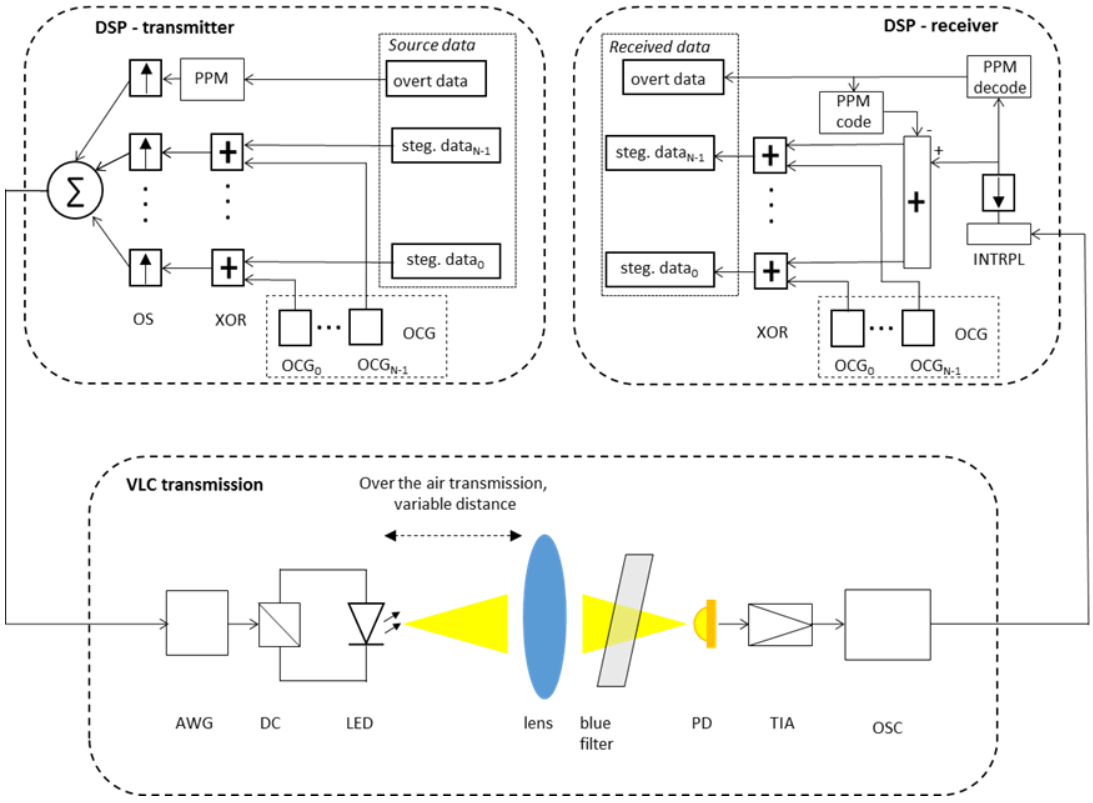
do danych będących w ruchu, tj. z wykorzystaniem możliwości, jakie stwarza dany kanał transmisyjny lub protokół – na przykład poprzez dodatkową modulację sygnału, poprzez zastosowanie nadmiarowych bitów w nagłówkach protokołu, czy też poprzez specyficzny rozkład czasowy pakietów. W przypadku steganografii zastosowanej do danych w ruchu wyróżnia się *kanał jawny (overt)* oraz *kanał ukryty (covert)*, tj. Zrealizowany przy pomocy techniki steganograficznej. W pracy [A4] zrealizowanej wspólnie z prof. dr hab. Krzysztofem Szczypiorskim z Instytutu Telekomunikacji Politechniki Warszawskiej zaproponowaliśmy techniki steganograficzne, jakie mogą zostać zastosowane w systemach VLC bazujących na standardzie IEEE 802.15.7 (ozwiązania te mogą być wykorzystane także w innych realizacjach VLC, niekoniecznie zgodnych z ww. standardem). Praca ta była pierwszym ujęciem tematyki steganograficznej dla systemów VLC. Zaproponowane przez nas metody obejmowały zarówno warstwę fizyczną (PHY), jak i kanałową (MAC), i obejmowały realizację ukrytego kanału poprzez:

- modyfikację mocy nadawania poziomów pośrednich w modulacji OOK (On-off keying),
- modyfikację długości pulsu w modulacji VPPM (Variable pulse position modulation),
- Wykorzystanie dodatkowych symboli konstelacji kolorów (w przypadku źródeł RGB),
- „nakładanie modulacji" – tj. sumowanie kanału jawnego modulowanego przy pomocy metod takich jak: OOK, PPM (Pulse-Position Modulation) z kanałem ukrytym modulowanym przy pomocy metod DS-CDMA – ta metoda opisana została dokładniej w następnym podrozdziale,
- przekazywanie danych w niekodujących wzorach służących do realizacji ściemniania (dimming) oraz unikania migotania, a także w sekwencjach pustych,
- ukrywanie danych w nagłówkach PHY IEEE 802.15.7 oraz MAC IEEE 802.15.7.

Dla większości opisanych wyżej technik steganograficznych oszacowano lub obliczono pojemność kanału steganograficznego tj. maksymalna liczbę bitów komunikatu ukrytego w stosunku do liczby bitów komunikatu jawnego. W pracy omówiona została też kwestia możliwości wykrycia zastosowania steganografii zaproponowanych typów.

Steganografia ma duże znaczenie praktyczne – wykorzystuje się ją między innymi w różnego rodzaju oprogramowaniu typu spyware oraz innych typach wrogiego oprogramowania i sprzętu, np. o charakterze szpiegowskim, które wymagają niezauważonej

transmisji przechwyconych danych na zewnątrz spenetrowanej domeny. Dlatego też analiza potencjału steganografii w VLC ma duże znaczenie zarówno teoretyczne, jak i praktyczne.



Rysunek 3 *– Blokowy schemat ogólny systemu LuxSteg. Oznaczenia modułów: PPM – Pulse Position Modulator, OS – oversampling, OCG – orthogonal code generation (for DS-CDMA), INTRPL – interpolation, AWG – arbitrary waveform generator, DC – driving circuit, PD – photo detector, TIA – transimpedance preamplifier, OSC – oscilloscope.*

Rozwinięciem koncepcji przedstawionych w pracy [A4] była praktyczna realizacja systemu steganografii VLC „LuxSteg", opisana w pracy [A6] (zrealizowanej wspólnie z: magistrem Pawłem Januszewskim, doktorem habilitowanym Grzegorzem Stępniakiem oraz profesorem Krzysztofem Szczypiorskim z Instytutu Telekomunikacji Politechniki Warszawskiej). Skonstruowany i opisany system teletransmisyjny (zilustrowany na rysunku 3) pozwalał na przesył danych jawnych z przepustowością 110 Mbps i jednoczesny przesył kanałem ukrytym o przepustowości około 1 Mbps. W kanale jawnym zastosowano modulację Pulse Position Modulation (PPM), zaś w kanale ukrytym DS-CDMA. Kanały jawny i ukryty były modulowane oddzielnie, a następnie analogowo sumowane w nadajniku. Modulacja CDMA (Code-Division Multiple Access) przypisuje poszczególnym źródłom korzystającym z tego samego kanału, tzw. sekwencje rozpraszające, dzięki którym odbiornik jednoznacznie identyfikuje przeznaczoną dla niego transmisję. SF (Spreading Factor), czyli współczynnik rozpraszania, jest podstawowym parametrem charakteryzującym kanał transmisji. W efekcie modulacja CDMA ma charakterystykę

podobną do sygnałów szumowych. Modulacja CDMA wykazuje się dużą odpornością na zewnętrzne i wewnętrzne (w tym odbicia multipath) zakłócenia oraz pozwala na łączenie niezależnych strumieni danych, co predestynuje ją do zastosowań steganograficznych – kanał ukryty może mieć relatywnie niską amplitudę. Kluczową miarą jakości transmisji steganografcznej jest jej niewykrywalność – im większa przepustowość kanału ukrytego w stosunku do jawnego, tym większe szanse wykrycia ukrytej transmisji. Inne istotne parametry to stopa błędów w kanale ukrytym oraz stopień degradacji kanału jawnego. W pracy opisano analitycznie oraz zweryfikowano eksperymentalnie związek tych miar z kluczowymi parametrami transmisji dla modulacji DS-CDMA SF (Spreading Factor) oraz jego amplitudy. Przyjęta metodyka klasyfikacji jakości realizacji steganografii była rozszerzeniem i kontynuacją oryginalnych koncepcji przedstawionych w pracy [A4]. Jak już argumentowano wyżej dla [A4], podobnie i ta praca, jako pionierskie zastosowanie steganografii w VLC, ma duże znaczenie zarówno teoretyczne jak i praktyczne.

Bezpieczeństwo VLC – podsumowanie

Obszar technologii i zastosowań VLC jest bardzo szeroko poruszany w literaturze. W przeglądowej pracy mojego autorstwa [A7] oszacowałem liczbę poświęconych mu artykułów naukowych na ponad 2000 (stan na początek roku 2020). Jednocześnie jednak liczba publikacji dotyczących bezpieczeństwa VLC była w tym samym okresie stosunkowo niewielka i wynosiła ponad 50. W poniższej tabeli (Tabela 1) podsumowuję kluczowe obszary badań związane z bezpieczeństwem VLC i mój w nich udział.

Lp.	Zagadnienie	Zakres w pracach własnych	Bibl.
1	Podstawowe aspekty: poufności, integralności i dostępności.	Jedna z pierwszych prac poświęcona tej tematyce. Nowatorskie, systematyczne ujęcie ww. zagadnień przy pomocy analizy ryzyka. Identyfikacja kluczowych zagrożeń dla róznorodnych scenariuszy zastosowań VLC.	A1, A2
2	Standard IEEE 802.15.7 – potencjalne podatności bezpieczeństwa warstw PHY i MAC, możliwość podsłuchiwania transmisji.	Kompleksowa analiza standardu pod względem bezpieczeństwa. Identyfikacja elementów standardu problematycznych w tym zakresie.	A1, A2, A4
3	Bezpieczeństwo fizyczne w ujęciu teorii informacji i teorioinformacyjny	W pracy przeglądowej A7 szeroko opisałem i podsumowałem teorioinformacyjne podejście do bezpieczeństwa VLC. W pracy A8	A5, A7, A8

	model kanału VLC, bezpieczne strefy komunikacji	wprowadziłem „dokładny" model kanału i porównałem go z przybliżonym.	
4	Beamforming i friendly jamming	W pracach odniosłem się do potencjału świetlnego BF dla zakłócania transmisji. Pierwsze podjęcie ww. kwestii w literaturze.	A1, A2
5	Wykorzystanie polaryzacji i koloru światła w aspektach zwiazanych z bezpieczeństwem.	-	-
6	Zakłócanie i podsłuchiwanie transmisji	Tematyka ta stanowi oś moich badań w zakresie VLC. Pierwszy systematyczne podjęcie ww. kwestii dla wszystkich schematów komunikacji VLC. Analityczne i symulacyjne badania różnorodnych scenariuszy.	A1, A2, A3, A5, A8
7	Steganografia w VLC	Pierwsza propozycja realizacji (na wielu poziomach sieci i z wykorzystaniem różnych mechanizmów) i pierwsza fizyczna realizacja.	A4, A6
8	Generowanie i zarządzanie kluczami kryptograficznymi z wykorzystaniem technik VLC.	Szeroko omówione w artykule przeglądowym.	A7
9	Bezpieczeństwo VANET (Vehicle Area Network – Sieci pojazdów (w ruchu)), bezpieczeństwo UWOC (Underwater Optical Communication) i inne.	-	-

Tabela 1 *– kluczowe obszary badań związane z bezpieczeństwem VLC.*

W ramach prowadzonych przeze mnie badań nad bezpieczeństwem systemów VLC powstało łącznie osiem publikacji naukowych z czego: dwie przy współudziale moich dyplomantów oraz dwie przy współudziale pracowników naukowych Instytutu Telekomunikacji Politechniki Warszawskiej.

4.4 Analiza ryzyka i klasyfikacja podatności systemów IoT

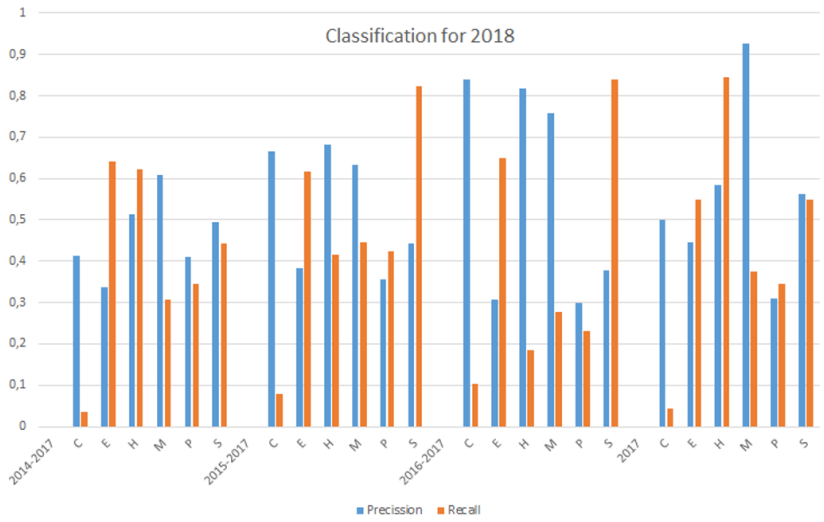
W latach 2017 – 2022 moje prace badawcze obejmowały też systemy IoT w zakresie infrastrukturalnym, tj. abstrahującym od konkretnego standardu lub technologii, a koncentrującym się na aspektach bezpieczeństwa IoT, rozumianych jako złożony układ wzajemnie powiązanych komponentów. W celu przybliżenia opisanej dalej tematyki poniżej syntetycznie przedstawiono założenia architektury infrastruktury IoT oraz użytą terminologię: punktem wyjścia dla moich prac była trójwarstwowa abstrakcyjna architektura IoT opisana np. w [2] i doprecyzowanej przeze mnie w [A9] obejmująca:

- *Warstwę wykonania i percepcji*, w skład której wchodzą sensory, inteligentne tagi, relatywnie proste systemy wykonawcze, bardziej złożone systemy domowe wchodzące w skład infrastruktury „SmartHome", a także przemysłowe systemy SCADA, które coraz częściej posiadają bezpośredni dostęp do internetu.
- *Warstwę sieciową* obejmującą przede wszystkim infrastrukturę pierwszej do czwartego poziomu stosu ISO OSI. W jej skład wchodzą systemy sieciowe i teletransmisyjne, zgodne ze standardami: Wi-Fi, 3G/LTE, Z-wave, ZigBee, 6LoWPAN, VLC, Ethernet, itd., wraz ze stosem protokół IPv4/v6 i warstwą transportu UDP/TCP.
- *Warstwę aplikacji chmurowych* służącą: gromadzeniu, integracji, zarządzaniu i analizie danych pochodzących z warstwy wykonania i percepcji.

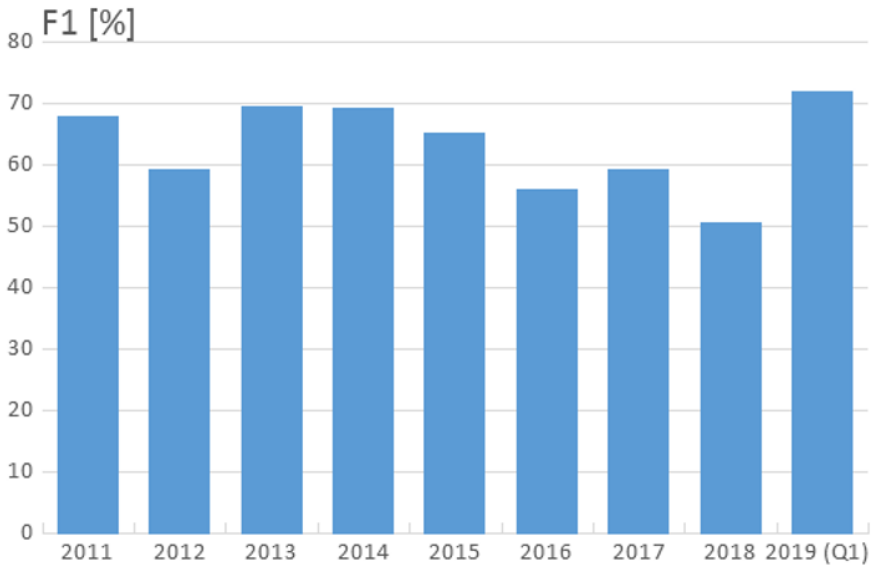
W pracy [A10] odniosłem się do kwestii bezpieczeństwa dwóch pierwszych warstw uniwersalnej architektury IoT, ze szczególnym uwzględnieniem warstw wykonania i percepcji. Błędy implementacyjne, głównie o charakterze softwarowym (tzw. podatności) są bardzo powszechne dla urządzeń i systemów IoT będących „na styku" ze środowiskiem fizycznym oraz użytkownikami – co roku raportowane są setki błędów związanych z bezpieczeństwem, a ich liczba rośnie. Przykładowo, liczba podatności zarejestrowanych w bazie CVE MITRE [15] związana z systemami, które możemy zaklasyfikować jako dotyczące IoT, w roku 2015 wyniosła 386, w roku 2017 – 813, zaś w roku 2018 – 1628. Częstym, a nawet dominującym problemem dotyczącym bazy CVE jest fragmentaryczność opisu zarejestrowanej podatności, dotyczy to w szczególnym stopniu systemów IoT[4].

[4] Baza CVE pierwotnie gromadziła prawie wyłącznie informacje dotyczące błędów czysto programowych, obecnie nadal większość wpisów koncentruje się na stronie programowej błędu, z pominięciem istotnych informacji o platformie sprzętowej.

Z uwagi na specyfikę CVE [16], znaczny odsetek rekordów tej bazy stanowią dane niepełne i/lub niejednoznaczne, np.: niejasna i/lub niepełna nazwa/typ/model urządzenia, niejasna lub niepełna natura błędu (informacja o tym, czego dokładnie dotyczy i czym się objawia). Problemy te powodują, że podmioty monitorujące bezpieczeństwo złożonej infrastruktury (duże przedsiębiorstwa, operatorzy telekomunikacyjni, dostawcy usług, firmy realizujące lub oferujące usługi typu SOC (Security Operations Center)) nie zawsze mogą pozyskać z tej bazy przydatne informacje. W pracy [A10] opisano automatyczny klasyfikator rekordów CVE opracowany specyficznie dla danych dotyczących systemów IoT. Klasyfikator wykorzystujący algorytm Support Vector Machine (SVM) [17, 18], na podstawie danych zaklasyfikowanych ekspercko określa klasę urządzenia, którego dotyczą nowe podatności zgłaszane do bazy. W wyniku wykonanego przeze mnie systematycznego przeglądu i „ręcznej" klasyfikacji reprezentatywnej próbki danych z CVE, obejmującej okres czterech lat (2014-2017) podatności zostały zaszeregowane do jednej z siedmiu kategorii: (1) rozwiązania konsumenckie (SOHO) (*H*), (2) systemy przemysłowe typu SCADA (*S*), (3) podzespoły i układy procesorowe (np. sterowniki) (P), (4) systemy sieciowe i infrastruktury (*E*), (5) konsumenckie urządzenia przenośne (*M*), (6) konsumencki sprzęt PC (*P*), (7) inne (pozostałe niedomowe urządzenia typu „appliance"). Zaproponowana metoda umożliwia określenie: adekwatności, stopnia zagrożenia i w pewnym zakresie ryzyka związanego z daną podatnością. Należy dodać, że praktyczna przydatność takiej automatycznej klasyfikacji jest niebagatelna, gdyż obecnie liczba podatności zgłaszana dziennie może wynosić kilkadziesiąt, a nawet kilkaset, a tych dotyczących IoT – kilkanaście, są to więc wielkości trudne do „ręcznego" zaklasyfikowania. Eksperymenty przeprowadzone z automatycznym klasyfikatorem pokazały, że jakość klasyfikacji mierzona standardowymi wskaźnikami: *precission, recall* oraz *F1*, wynosiła od 65% do 73% (dla ważonego parametru precision). Wyższą dokładność klasyfikacji osiągnięto dla liczniejszych klas. Przykładowe wyniki z pracy [A10] przedstawiono na rysunkach 4 i 5, które ilustrują odpowiednio: wyniki klasyfikacji dla różnych klas urządzeń opisanych literami C, E, H, M, P, S na podstawie „ręcznie" poklasyfikowanych danych z lat wcześniejszych, oraz sumaryczną wartość parametru *F1*dla całego zbioru danych.



Rysunek 4 *– Wyniki klasyfikacji podatności z bazy CVE za pomocą algorytmu SVM, parametry precission oraz recall (na podstawie pracy [A10]).*



Rysunek 5 *– Wyniki klasyfikacji podatności z bazy CVE za pomocą algorytmu SVM, ważony dla wszystkich klas parametr F1 dla kompletu danych (na podstawie pracy [A10]).*

W pracy [A11] opisano badania powtórzone z zastosowaniem klasyfikatora zrealizowanego przy pomocy sieci neuronowej, co poprawiło wyniki w stosunku do klasyfikatora SVN – osiągnięto ważoną wartość miary precission z przedziału 73-78%. Prace [A10, A11] były pierwszymi publikacjami odnoszącymi się do automatycznej klasyfikacji podatności Internetu Rzeczy. Praca [A10]

była cytowana (wg. Google Scholar) 40 razy. Analiza wybranych referencji, ograniczonych do prac, które ukazały się w "punktowanych" czasopismach oraz konferencjach wykazała:

- Prac opisujących oryginalne: rozwiązanie, technologię, protokół lub system: 6
- Prac z dziedziny modelowania zagrożeń lub podatności IoT: 5
- Prac z dziedziny analizy zagrożeń: 5

Wyżej wymienione referencje ukazały się m.in. w: Computer Networks; Computers, Software, and Applications Conference (COMPSAC) IEEE; Foundations and Practice of Security; Journal of Information Processing Systems; IEEE International Conference on Cyber Security and Resilience; Journal of Intelligent Information Systems; Proceedings of the 2022 ACM Conference on Computer and Communications Security i były cytowane łącznie 123 razy.

Jednym z obszarów mojej działalności była także analiza ryzyka dla systemów informatycznych – była ona punktem wyjścia do analizy bezpieczeństwa systemów VLC (co opisałem wyżej), inne aspekty moich prac odnoszących się do analizy ryzyka wymieniłem w załączonym Wykazie. Analiza ryzyka była też punktem wyjścia do stworzenia opartego na niej oraz pojęciu zaufania (*trust*) architektury IoT [A9]. Architektura ta bazuje na opisanym wcześniej uniwersalnym modelu trójwarstwowym, jej istotą jest podejmowanie decyzji lokalnych (w obrębie węzła warstwy percepcji) na podstawie globalnej oceny ryzyka. Przykładem lokalnej decyzji jest podjęcie lub zaniechanie wykonania w węźle transakcji, która może mieć charakter „niskopoziomowy", np. dotyczącej przekierowania lub odrzucenia trasowanego pakietu danych. Proponowany algorytm realizacji lokalnych transakcji funkcjonuje w zarysie w następujący sposób:

1. Obliczane jest zaufanie (*reliabiliy trust*) w stosunku do węzłów, z którymi lub na rzecz których będzie realizowana transakcja. Wartość ta obliczana jest na podstawie historii wcześniejszych transakcji lub, przy ich braku, przyjmowana jest wartość domyślna.
2. Obliczany jest zysk (*gain*) z wykonania (lub zaniechania) danej transakcji, zysk obliczany jest na podstawie zaufania oraz dodatkowych parametrów lokalnych (np. dostępnego poziomu energii w baterii). Zysk modelowany jest nie jako pojedyncza wartość, lecz jako zmienna losowa (zwykle o rozkładzie innym niż normalny). Posiłkujemy się też teorią użyteczności (*utility*), w której zysk nie musi być funkcją liniową.

3. Obliczane jest ryzyko wykonania (lub zaniechania) danej transakcji. Bezpośrednie wyznaczenie ryzyka w czasie rzeczywistym nie może być wykonane lokalnie, ze względu na ograniczenia mocy węzłów i jednocześnie na stosunkowo skomplikowane obliczenia na rozkładach zmiennych losowych. Zamiast tego ryzyko określane jest na podstawie gotowych sparametryzowanych tabel typu „lookup" generowanych na poziomie chmurowym, na podstawie cząstkowych danych pozyskiwanych z węzłów.
4. Transakcja wykonywana jest (lub nie), gdy obliczony poziom ryzyka nie przekracza ustalonej wartości progowej.

W pracy zaproponowano też realizację schematu komunikacji umożliwiającego prostą implementację powyższego algorytmu przy pomocy protokołu MQTT (MQ Telemetry Transport).

Podsumowując: proponowana architektura pozwala na szybkie (nisko kosztowe w sensie obliczeniowym) podejmowanie lokalnych (w węźle) decyzji na podstawie globalnej oceny ryzyka wykonywanej na poziomie chmurowym.

4.6 Podsumowanie

Moje prace przedstawione w niniejszym autoreferacie dotyczyły bezpieczeństwa systemów Internetu Rzeczy. Dziedzina IoT od kilkunastu lat pozostaje jednym z głównych obszarów innowacji w zakresie informatyki, zarówno pod względem teoretycznym jak i praktycznym. Rozwój nowych technologii i protokołów komunikacji – głównie bezprzewodowych, przyczynia się do rozwoju złożonych systemów IoT (np. sieci sensorów), co z kolei napędza rozwój nowych: modeli komunikacji, koncepcji integracji warstw oraz zabezpieczenia danych w spoczynku i w ruchu.

Zaproponowane przeze mnie metody i rozwiązania cechuje wyraźnie zaznaczony wkład oryginalny oraz czytelne, przejrzyste, logiczne i przekonujące uzasadnienie teoretyczne leżące u podstaw wprowadzanych innowacji. Dla technologii VLC oryginalne i nie występujące wcześniej w literaturze elementy tego wkładu są następujące:

1. Zastosowanie systematycznej analizy ryzyka jak punktu wyjścia do obiektywnej oceny poziomu bezpieczeństwa komunikacji VLC we wszystkich stosowanych w praktyce scenariuszach środowiskowych [A1, A2].
2. Teoretyczna, symulacyjna i eksperymentalna weryfikacja możliwości przeprowadzenia ataku na systemy VLC. Rozbudowa podstawowego ("Gausowskiego") modelu symulacyjnego do modelu "dokładnego" i porównanie obydwu modeli [A3, A5, A8].
3. Eksploracja pola bezpieczeństwa systemów VLC jakim jest steganografia – przedstawienie szerokiego zakresu nowych dla tego obszaru scenariuszy teoretycznych oraz praktyczna weryfikacja w postaci skonstruowanego i przetestowanego systemu sprzętowego [A4, A6].
4. Praca [A7] stanowi podsumowanie moich badań w zakresie VLC, systematyzuje i wyczerpująco przedstawia wszystkie kluczowe aspekty bezpieczeństwa systemów posługujących się w komunikacji światłem widzialnym. Na uwagę zasługuje wysoka liczba cytowań tej pracy wynoszącą 70 (wg Google Scholar).

Wyżej wymienione prace dotyczące różnych aspektów bezpieczeństwa systemów VLC osiągnęły łącznie ponad 180 cytowań (wg Google Scholar).

Drugi z obszarów moich badań związanych z IoT dotyczył kwestii bezpieczeństwa dwóch pierwszych warstw uniwersalnej architektury IoT, ze szczególnym uwzględnieniem warstwy wykonania i percepcji. Prace [A10, A11] były pierwszymi w znanej mi literaturze publikacjami odnoszącymi się do automatycznej klasyfikacji podatności Internetu Rzeczy, warto nadmienić, że osiągnęły łącznie ponad 40 cytowań (wg Google Scholar). Zaproponowałem też metodę realizacji transakcji w warstwie percepcji bazującą na ocenie ryzyka i zaufaniu [A9].

Analiza cytowań, w szczególności dla: [A1, A2, A5, A7, A10] wykazuje, że w znaczącym stopniu stały się one dla środowiska bazą do dalszych prac i rozwoju technologii, związanych z bezpieczeństwem IoT.

4.7 Wykaz przywoływanych pozycji

[1] Ding, J., Nemati, M., Ranaweera, C., Choi, J. IoT connectivity technologies and applications: A survey. IEEE Access, 8, 67646-67673. 2020.

[2] Neshenko, N., et al., Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733. 2019.

[3] Antonakakis, M., et al., Understanding the Mirai botnet. In 26th USENIX security symposium (USENIX Security 17) (pp. 1093-1110). 2017.

[4] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B., A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743. 2019.

[5] Pathak, . H. , Feng, X. . Hu, P., Mohapatra, P.,"Visible light communication, networking, and sensing: A survey, potential and challenges," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2047–2077, Fourthquarter 2015.

[6] Tanaka, Y. Haruyama, S., Nakagawa, M.,"Wireless optical transmissions with white colored led for wireless home links," in Personal,Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on, vol. 2. IEEE, pp. 1325–1329, 2000.

[7] Langer, K.-D., et al., "Optical wireless communications for broadband access in home area networks," in Transparent Optical Networks, 2008. ICTon 2008. 10th Anniversary International Conference on, vol. 4, pp. 149–154., IEEE 2008.

[8] IEEE. 2011. IEEE standard for local and metropolitan area networks–part 15.7: Short-range wireless optical communication using visible light", IEEE Std 802.15.7-2011, https://standards.ieee.org/findstds/standard/802.15.7-2011.html

[9] Mostafa, A., & Lampe, L., Physical-layer security for indoor visible light communications,'' In Proceedings IEEE ICC 2014—optical networks and systems, 2014.

[10] Conti, J.P. , "What you see is what you send," Engineering & Technology, pp. 66-67, 2008.

[11] T. Komine and M. Nakagawa, Fundamental analysis for visible-light communication system using LED lights, IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 100–107, 2004.

[12] Jaesang Cha, et al., Home-page document for LED-ID: LED-ID Related Technical Features and Applications, online: https://mentor.ieee.org/802.15/dcn/15/15-15-0410-00-007a-home-page- document-for-led-id-led-id-related-technical-features-and-applications.pptx, 2015.

[13] The 7th Framework Programme funded European Research and Technological Development from 2007 until 2013; Internet of Things and Future Internet Enterprise Systems; http://cordis.europa.eu/fp7/ict/enet/projects_en.html, last accessed 2017/05/10

[14] Mondal, S. C., Prabhu, S. *U.S. Patent No. 11,317,423*. Washington, DC: U.S. Patent and Trademark Office. (2022).

[15] MITRE, CVE Common Vulnerabilities and Exposures database, online: https://cve.mitre.org/ last accessed: 29.11.2023 (2020)

[16] NIST, Official Common Platform Enumeration (CPE) Dictionary, https://csrc.nist.gov/projects/security-content-automation-protocol/, last accessed: 02.01.2020. (2020)

[17] Vapnik, V.: Statistical Learning Theory. John Wiley & Sons, New York, NY. 1998.

[18] Liu, Z., Lv, X., Liu, K., & Shi, S. . Study on SVM compared with the other text classification methods. In Second International Workshop on Education Technology and Computer Science (Vol. 1, pp. 219-222). IEEE. 2010.

4.8 Opis pozostałej działalności naukowo-badawczej

Wstęp

Innym, choć w pewnym zakresie powiązanym z przedstawionym wyżej cyklem, obszarem mojej działalności są technologie związane z rozwojem aplikacji chmurowych. W sekcji 5 wymieniłem i krótko opisałem projekty wdrożeniowe obejmujące tą tematykę, w których uczestniczyłem, a które realizowane były wspólnie z podmiotami innymi niż moja macierzysta uczelnia. Dotyczy to w szczególności **Europejskiego projektu NeuroMath** obejmował pionierskie w pierwszej dekadzie XXI w. stworzenie sieci powiązanych portali specjalizowanych do przechowywania i udostępniania oprogramowania, zbiorów danych i publikacji z zakresu czynności elektrycznej mózgu. Projekt ten można zakwalifikować jako jedną z pierwszych prób stworzenia sfederowanej sieci usług chmurowych dla zastosowań biofizycznych.

Podobny charakter miały też projekty bazujące na oprogramowaniu WWW-ISIS opisane niżej związane z tworzeniem repozytoriów danych dostępnych za pośrednictwem technologii webowych:

Oprogramowanie WWW-ISIS

W ramach współpracy z zespołem prof. Henryka Rybińskiego z Instytutu Informatyki Politechniki Warszawskiej uczestniczyłem w tworzeniu i rozwoju oprogramowania WWW-ISIS oraz WEBLIS – platformy zgodnej z systemem CDS-ISIS (opracowanym oryginalnie przezUNESCO) służącej do realizacji systemów bibliotecznych (katalogowych). Oprogramowanie WWW-ISIS zostało wdrożone w licznych organizacjach NGO oraz agendach Organizacji Narodów Zjednoczonych, między innymi w: FAO, UNIDO, UNESCO, IUCUN – łącznie w latach 2001 – 2009: ponad 30 wdrożeń. W samym FAO w w.w. okresie wdrożono następujące instancje tego oprogramowania: FAOBIB – katalog biblioteki głównej, FAODOC - bibliografia prac FAO, FAOLEX, AGRIS, AGROVOC, ASFA-ISIS, ASFA thesaurus. System WEBLIS był wdrożony w: WFP, ICCROM, IFAD (agendy ONZ), IDLO (NGO działające w Rzymie), IFRC (The International Federation of Red Cross), EFSA (The European Food Safety Authority). System wdrożono też w kilku instytucjach krajowych – do dzisiaj (09/2024) działa jego instalacja w IBLES (Instytut Badawczy Leśnictwa). Opracowane przez nasz zespół oprogramowanie, które przez niektóre agendy ONZ było swobodnie dystrybuowane, doczekało się też innych wdrożeń oraz publikacji i opracowań, przeglądowe opracowanie wdrożeń i potencjału znaleźć można np. w publikacji [**B1**], zaś częściowe podsumowanie prac wykonanych dla FAO znajduje się w [**B2**]. Kwerenda wykonana przy pomocy Google Scholar zwraca 8750 pozycji dla

"WWWISIS" oraz 234 pozycje dla "WEBLIS". Podsumowując – warto zaznaczyć, że oprogramowanie WWWISIS było projektem nowatorskim na skalę światową, gdyż w przeciwieństwie do powszechnie funkcjonujących w pierwszej dekadzie XXI w. zamkniętych systemów tego typu, funkcjonujących jako natywne aplikacje systemów mainframe, Unix, Windows (a nawet MS-DOS), WWW-ISIS stosowało otwarte standardy i technologie internetowe, co znacząco redukowało koszt wdrożenia i utrzymania systemu. Pionierskim rozwiązaniem było też opracowany dla FAO wariant tego samego oprogramowania, pozwalający na uruchamianie aplikacji bez dostępu do sieci (przewidziany dla krajów rozwijających się pozbawionych nierzadko infrastruktury internetowej). Oprogramowanie WWW-ISIS i zbudowane na nim systemy oraz usługi znacząco przyczyniły się do rozwoju systemów bibliotecznych w skali światowej.

WWW-ISIS na platformach Lucene i MongoDB

Uczestniczyłem w projekcie realizowanym przez Instytut Informatyki Politechniki Warszawskiej dla Food and Agriculture Organization of the United Nations (FAO) związanym z dalszym rozwojem oprogramowania WWW-ISIS (2009 – 2011). W tworzonym oprogramowaniu zostały zastosowanie narzędzia Lucene i MongoDB, co było jednym z pierwszych w świecie wdrożeń nierelacyjnych baz danych w tej dziedzinie i tej skali. Oprogramowanie zostało wdrożone w FAO (system FAOLEX), a nieco później w International Union for the Conservation of Nature (IUCN) – bazy FAOLEX i ECOLEX oraz w innych instytucjach (IFRC, EFSA).

Skalowalność mikroserwisów

Aspektu skalowalności technologii chmurowych dotyczy praca [**B3**], zrealizowana w roku 2021 wspólnie z doktorem Adamem Przybyłkiem i magister Anną Ojdowską z Wydziału Telekomunikacji i Informatyki Politechniki Gdańskiej. Dokonano kompleksowego rankingu wydajności i skalowalności aplikacji chmurowych wykorzystujących mikroserwisy, ze szczególnym uwzględnieniem finansowych kosztów eksploatacji aplikacji wykonanych w różnych technologiach i uruchamianych w chmurze publicznej głównych dostawców. W pracy przeanalizowano dwie wzorcowe aplikacje napisane zarówno z wykorzystaniem języka Java jak i C# oraz stworzone w dwóch wariantach każda – monolitycznym oraz bazującym na mikroserwisach. W każdym z ośmiu wynikowych wariantów przeanalizowano wydajność oraz finansowy koszt dla platformy: lokalnej (tj. nie chmurowej), Azure Spring Cloud oraz Azure App Service. W wyniku prowadzonych pomiarów uzyskano wartościowe i zróżnicowane rezultaty zależne od

charakteru aplikacji (zorientowana na obliczenia, kontra zorientowana na komunikację), rodzaju skalowania chmurowego (wertykalne i horyzontalne) oraz języka i środowiska programowania. O znaczeniu powyższej pracy świadczy liczba cytowań, która wynosi obecnie 140 (maj 2024).

Fuzzing systemów TEE

Ostatnim (w sensie chronologicznym) obszarem moich zainteresowań i badań naukowych jest stosunkowo młoda dziedzina związana z bezpieczeństwem i testowaniem oprogramowania nazywana „fuzzingiem" (ang.: *fuzzing, fuzz-testing*). Fuzzing to technika testowania oprogramowania, służąca do lokalizacji błędów, która polega na automatycznym generowaniu pseudolosowych, nieoczekiwanych i/lub niepoprawnych danych wejściowych w celu wykrycia potencjalnych problemów w testowanym kodzie. Fuzzing pozwala zidentyfikować nieprawidłowe zachowania programu takie jak: załamania, wycieki pamięci, nieoczekiwane wyjątki oraz luki bezpieczeństwa. Fuzzing początkowo stosowany był do testowania programów przyjmujących dane wejściowe w postaci pliku lub wektora. Trudniejszym w realizacji zagadnieniem jest stosowanie fuzzingu do testowania systemów operacyjnych, a ściśle – systemowego API. W pracy [**B4**] zrealizowanej wspólnie z moim dyplomantem, Panem Michał Szaknisem, przedstawiliśmy nowatorską metodę zastosowania technik fuzzingu do testowania bezpieczeństwa systemów TEE[5]. Nowatorski charakter w.w. pracy polega na wykorzystaniu jednorodnego opisu testowanego API w dwóch celach:

(1) Realizacji tzw. strukturalnego fuzzingu (ang.: *structured fuzzing*), polegającego na generowaniu takich danych testowych, które nie zostaną odrzucone przez API na wstępnym etapie weryfikacji argumentów i i jednocześnie wygenerowania logicznie poprawnej sekwencji wywołań systemowych (przykładowo: przy testowaniu API systemu plików, należy wywołać funkcję *open()*, a następnie funkcję *read()* oraz przekazać do funkcji *read()* zwrócony przez *open()* uchwyt pliku; sekwencja odwrotna, tj. *read()*, a następnie *open()* nie ma sensu i nie stanowi skutecznego testu).

(2) Automatycznym przekształceniu testów kodu jednostkowych w wektory inicjujące pseudolosowe dane testowe. Metody stosowane do tej pory stosowały zazwyczaj podejście

[5] Systemy TEE (Trusted Execution Environment) to wyizolowane, bezpieczne środowiska wykonawcze, zaprojektowane w celu ochrony wrażliwych danych i procesów przed nieuprawnionym dostępem, nawet w przypadku kompromitacji głównego systemu operacyjnego. Przykładowe platformy sprzętowe TEE to np.: Intel SGX i ARM TrustZone. Są one wykorzystywane w aplikacjach wymagających wysokiego poziomu bezpieczeństwa, np. w kryptografii, są też bazą sprzętową dla wielu systemów IoT.

hybrydowe, łączace pewną formę formalnego opisu testowanego API z dynamicznie zbieranym śladem wykonania uzyskanym poprzez instrumentację kodu źródłowego.

Podejście opisane w pracy [B4] zostało zaimplementowane i przetestowane w systemie operacyjnym OP-TEE przeznaczonym dla platformy ARM-Trustzone. Opracowane środowisko fuzzingu bazuje na języku programowania Rust, a dzięki mechanizmowi tzw. makr proceduralnych tego języka, udało się bardzo znacząco zredukować złożoność kodu i stworzyć narzędzie znacznie bardziej uniwersalne, niż dotychczas stosowane. Innym nowatorskim aspektem opisywanej pracy jest zastosowanie wirtualizatora QEMU, który został rozbudowany o dodatkowe mechanizmy odtwarzania stanu testowanego systemu operacyjnego. Dzięki temu możliwe było wygenerowanie różnych wariantów fuzzingu – z oraz bez odtwarzania stanu systemu między kolejnymi rundami testowania. Podejście takie ma dość istotne znaczenie, gdyż różne warianty odtwarzania stanu systemu mają bardzo znaczący wpływ na wydajność i konsumpcję zasobów podczas testów. Zebrane dane jakościowe i ilościowe dotyczące efektywności w lokalizacji błędów oraz szybkości ich wykrywania także wykazują znaczny potencjał stworzonej metodyki oraz narzędzia[6].

Książka monograficzna „Systemy poczty elektronicznej – standardy, architektura bezpieczeństwo"

Mimo rozpowszechnienia się w drugiej dekadzie XXI w. różnego rodzaju portali służących do wymiany informacji (dedykowanych jak i uniwersalnych), systemów obiegu dokumentów funkcjonujących wewnątrz struktury organizacyjnej oraz innych systemów komunikacji elektronicznej, poczta elektroniczna pozostaje podstawowym środkiem wymiany informacji zarówno wewnątrz organizacji jak i między nimi. Z uwagi na krytyczne znaczenie systemów e-mail kluczowego znaczenia nabiera jej bezpieczeństwo. Książka mojego autorstwa [**B5**] przedstawia kompletny obraz funkcjonowania systemów e-mail przedstawionych w dużej mierze z punktu widzenia bezpieczeństwa. Pozycja ta (w przeciwieństwie do innych, które pojawiły się na rynku w ciągu ostatnich dwóch dekad) nie stanowi opisu lub podręcznika użytkownika konkretnych programów, czy też systemów (komercyjych lub darmowych), a jest kompletnym i systematycznym przeglądem protokołów i standardów reprezentacji

[6] Z uwagi na zaadresowanie aspektów bezpieczeństwa oraz na platformy sprzętowe, których ona dotyczy, praca ta stanowi kontynuację moich badań związanych z technologiomi IoT, jedna z uwagi na uwarunkowania czasowe oraz początkową fazę analizy tematyki, praca ta nie została dołączona do cyklu.

i kodowania danych na których bazują współczesne systemy poczty elektronicznej. Publikacja ta ma więc charakter monograficzny.

W książce przedstawiono podstawowe standardy, na których bazują systemy e-mail: protokoły ESMTP[7], POP, IMAP oraz zasady konstrukcji wiadomości e-mail, tj. przede wszystkim standard MIME. Opisano też szczegółowo standardy S/MIME i PGP pozwalające na realizację zabezpieczenia przesyłanych wiadomości w trybie "end-to-end". Jako, że S/MIME bazuje na rodzinie standardów PKI, omówiono też technologię wybranych standardów związanych z kryptografią asymetryczną stosowanych w systemach poczty, tj. standardy PKCS i CMS oraz koncepcję i zasady funkcjonowania centrów certyfikacji (CA) oraz język ASN.1 i kodowanie BER.

W ramach dyskusji poświęconej bezpieczeństwu omówiono takie potencjalne konsekwencje ataków na systemy poczty elektronicznej jak: odpowiedzialność prawna, straty wizerunkowe, utratę produktywności oraz konsekwencje dla użytkowników indywidualnych. Omówiono dokładnie techniczne źródła ryzyka związane z utratą lub uszkodzeniem danych e-mail: zaniedbania i świadome działania pracowników; zagrożenia zewnętrzne; szpiegostwo przemysłowe i państwowe. Przedstawiono analizę ryzyka i koszty zabezpieczenia systemów pocztowych. Dużo miejsca poświęcono technicznej tematyce ochrony użytkowników poczty elektronicznej, tj: detekcji złośliwego kodu, eliminacji spamu oraz uniwersalnej filtracji treści obejmującej analizę załączników, analizę leksykalną i inne.

W ostatnim rozdziale przedyskutowana została architektura systemów e-mail, ze szczególnym uwzględnieniem instalacji dużej skali, tj. obejmujących wydzielone serwery brzegowe i filtrujące, dedykowany urząd pocztowy (PO) oraz usługi katalogowe LDAP.

Podsumowując, pozycja ta w wyczerpujący sposób omawia zagadnienia związane z funkcjonowaniem systemów poczty elektronicznej ze szczególnym uwzględnieniem szerokiego spektrum kwestii bezpieczeństwa zarówno ze strony teoretycznej jak i praktycznej.

Przywoływane pozycje

[**B1**] Blinowski, G., Rybiński, H., Ramsza, T., & Kustra, T. (2013), *Alpha-ISIS–web-and cloud-oriented information storage and retrieval environment. Information Systems Architecture and Technology,* Proc. of the 34th International Conference ISAT (Information Systems Architecture and Technology) 2013; Wrocław University of Technology, Ed. L. Borzemski, et al.; Avaiable in: Information Systems Architecture

[7] Skróty w tej oraz kolejnych sekcjach rozwinięte są w dodatku zamiejszczonym na końcu autorteferatu.

and technology, Intelligent Information systems, Knowledge Discovery, Bigh Data and High Performance Computing; ed. A. Górski, Oficyna Wydawnicza Politechniki Wrocławskiej; pp. 111, ISBN 978-83-7493-800-6. 2013.

[B2] Rybiński, H., Blinowski, G. J., & Ramsza, T. (2011). *α-WWW/ISIS Technical Reference Manual v. 1.0* (No. 7/2011). The Institute of Computer Science. 2011.

[**B3**] Blinowski, G., Ojdowska, A., & Przybyłek, A., *Monolithic vs. microservice architecture: A performance and scalability evaluation.* IEEE Access, 10, 20357-20374. 2022.

[**B4**] Blinowski, G., Szaknis, M., *Fuzzing Trusted Environments with Rust,* Computers & Security, ___, 2024. (Artykuł przyjęty, ukaże się w listopadzie 2024)

[**B5**] Blinowski G., *Systemy poczty elektronicznej. Standardy, architektura, bezpieczeństw*; (Książka), BTC 2012, ISBN 978-83-60233-83-2. 2012.

4.9 Pełna bibliografia (po doktoracie)

— Blinowski, G., Durka, P., & Spasiński, A., *Inter-neuro: from chaos to neuroinformatics knowledge base*. Journal of Medical Informatics & Technologies, 7. 2004.

— Durka, P. J., Blinowski, G. J., Klekowicz, H., Malinowska, U., Kuś, R., & Blinowska, K. J. (2009). *Information infrastructure for cooperative research in neuroscience*. Computational Intelligence and Neuroscience, 2009.

— Blinowski G., *Systemy poczty elektronicznej. Standardy, architektura, bezpieczeństw*; (Książka), BTC 2012, ISBN 978-83-60233-83-2. 2013.

— Blinowski, G., Ciechańska, K., *KCMail - wydajny filtr protokołu SMTP*; Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne 7/2013 ISSN 1230-3496. 2013.

— Blinowski, G., Rybiński, H., Ramsza, T., & Kustra, T. (2013), *Alpha-ISIS–web-and cloud-oriented information storage and retrieval environment. Information Systems Architecture and Technology*, Proc. of the 34th International Conference ISAT (Information Systems Architecture and Technology) 2013; Wrocław University of Technology, Ed. L. Borzemski, et al.; Avaiable in: Information Systems Architecture and technology, Intelligent Information systems, Knowledge Discovery, Bigh Data and High Performance Computing; ed. A. Górski, Oficyna Wydawnicza Politechniki Wrocławskiej; pp. 111, ISBN 978-83-7493-800-6. 2013.

— Blinowski, G., Kamiński, M., & Wawer, D., *Trans3D: a free tool for dynamical visualization of EEG activity transmission in the brain*. Computers in Biology and Medicine, 51, 214-222. 2014.

— Blinowski, G., Pieczerak, T., *Układ Raspberry Pi jako uniwersalna platforma mikro-appliance do zastosowań sieciowych i bezpieczeństwa*. Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne, nr 7/2014.

— Blinowska K., Kaminski M., Baccala, L., Sameshima K., Blinowski G., E*stimation of Effective Connectivity from Electrophysiological Time Series* (A Special Sessions Tutorial), Proceedings - Type II, Web Inteligence Congress, 11-14 August 2014, Warsaw, Poland

— Blinowski, G., *Sieci VLC i ich bezpieczeństwo*; Konferencja: Secure 2014, Warszawa, 22-23.10.2014 Organizator: NASK, Cert.pl. 2014.

— Blinowski, G., *Security issues in visible light communication systems*, IFAC-PapersOnLine, Vol. 48, No. 4, pp. 234 – 239, 2015, Elsevier
— Blinowski, G., *Practical aspects of physical and MAC layer security in visible light communication systems*, International Journal of Electronics and Telecommunications, Vol. 62, No. 1,pp. 7 – 13. 2016.
— Blinowski, G., Kmieciak, A., *Modelling and evaluation of a multi-tag LED-ID platform*. Proc. Federated Conference on Computer Science and Information Systems (FEDCSIS), Gdańsk, Poland, 11 - 14 September, 2016.
— Blinowski, G., Szczypiorski, K., *Steganography in VLC Systems*, Journal of Universal Computer Science, ISSN 2081-8491; Vol. 23, No. 5, pp. 454-478, 2017
— Blinowski, G., *The feasibility of launching rogue transmitter attacks in indoor visible light communication networks*. Wireless Personal Communications, Vol. 97, pp. 5325-5343,2017, Springer US. 2017.
— Blinowski, G., Januszewski, P., Stępniak, G., Szczypiorski, K.. *LuxSteg: First practical implementation of steganography in VLC*, IEEE Access,Vol. 6, pp. 74366-74375, IEEE. 2018.
— Blinowski, G., *Risk-Based Decision Making in IoT Systems*. Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017. Part I / Borzemski Leszek, Świątek Jerzy, Wilimowska Zofia (*red.*), Advances in Intelligent Systems and Computing, vol. 655, Cham, Springer, s.230-241, ISBN 978-3-319-67219-9. 2018.

Blinowski, G.: *Security of visible light communication systems—A survey*, Physical Communication, Vol. 34, pp. 246-260, Elsevier. 2019.
— Blinowski, G.; Mościcki, A., *Comparing Gausian and exact models of malicious interference in VLC systems*, International Journal of Electronics and Telecommunications, Vol. 65. 2019.
— Blinowski, G., Piotrowski, P., *CVE based classification of vulnerable IoT systems*; International Conference on Dependability and Complex Systems; pp. 82-93, Springer. 2020.
— Blinowski, G. J., Piotrowski, P., Wiśniewski, M. (2021). *Comparing Support Vector Machine and Neural Network Classifiers of CVE Vulnerabilities*; Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021), pages 734-740, ISBN: 978-989-758-524-1

— Blinowski, G., Ojdowska, A., & Przybyłek, A., *Monolithic vs. microservice architecture: A performance and scalability evaluation.* IEEE Access, 10, 20357-20374. 2022.

5. Informacja o wykazywaniu się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.

W ramach międzynarodowego projektu „**NeuroMath**" (inicjatywa Science Forum OECD), którego uczestnikiem były uczelnie z krajów UE, nadzorowałem i uczestniczyłem bezpośrednio w wytworzeniu oprogramowania systemu portalowego. Efektem projektu, realizowanego w okesie 05/2007 – 05/2011, było m.in. stworzenie platform internetowych: „Interneuro" oraz „Egg.pl" będących otwartym repozytorium: oprogramowania, zbiorów danych i publikacji z zakresu czynności elektrycznej mózgu (EEG, LFP, ERP). W w.w. portalach zaimplementowałem pionierskie wówczas rozwiązania informatyczne z zakresu wyszukiwania opartego na semantyce oraz między-portalowej wymiany danych bazującej na standardzie XML-RPC. Projekt był finansowany przez międzynarodowy grant COST Action BM0601 "NeuroMath" oraz grant Ministerstwa Nauki i Szkolnictwa Wyższego nr 119/N-COST/2008/0). Założenia i informatyczne i rezultaty projektu opisano w pracach [**C1, C2**], których jestem współautorem. W ramach projektu Interneuro bezpośrednio współpracowałem z zespołem badawczym z Zakładu Fizyki Medycznej Wydziału Fizyki Uniwersytetu Warszawskiego (obecnie Zakład Fizyki Biomedycznej) (prof. Piotr Durka) oraz Uniwersytetem Sapienza w Rzymie (kontakt: prof. Fabio Babiloni). Rola w projekcie: współwykonawca, wykonanie i koordynacja prac nad w.w. portalami.

Zarządzałem projektem finansowanym przez PARP (Polska Agencja Rozwoju Przedsiębiorczości), którego beneficjentem był **Instytut Energii Atomowej POLATOM**. Celem projektu było opracowanie założeń dla oprogramowania edukacyjnego w zakresie energetyki jądrowej (kontakt: dr Bogna Laurikainen). Projekt został zrealizowany w roku 2009. Rola w projekcie: współwykonawca

Zarządzałem projektem „**Trans3D**" (okres: 2012 – 2014), którego celem było stworzenie oprogramowania służącego do trójwymiarowej wizualizacji mózgowych potencjałów wywołanych na czaszce i/lub korze mózgowej pacjentów. Projekt realizowany

był we współpracy z Zakład Fizyki Medycznej Wydziału Fizyki Uniwersytetu Warszawskiego (kontakt: dr hab. prof. ucz. Maciej Kamiński). Wytworzone oprogramowanie zostało udostępnione w domenie publicznej i było następnie wykorzystane w szeregu prac badawczych. Oprogramowanie Trans3D opisane w pracy [**C3**] (Praca uzyskała nagrodę wydawcy: „Top 10 Papers of the Year 2014"). Byłem też współautorem tutorialu przygotowanego na konferencję poświęconą tematyki analizy sygnałów z wykorzystaniem tego narzędzia [**C4**].

Opisany w poprzednim punkcie program został pod moim nadzorem zmodyfikowany do celów wizualizacji potencjałów wywołanych u zwierząt. Projekt realizowano na zamówienie Prof. Wioletty Waleszczyk z Instytutu Biologii Doświadczalnej im. M. Nenckiego w Warszawie (2015- 2017).

Bibliografia

[C1] Blinowski, G., Durka, P., & Spasiński, A., *Inter-neuro: from chaos to neuroinformatics knowledge base*, Journal of Medical Informatics & Technologies, *7*. 2004.

[C2] Durka, P. J., Blinowski, G. J., Klekowicz, H., Malinowska, U., Kuś, R., & Blinowska, K. J., *Information infrastructure for cooperative research in neuroscience*,

[C3] Blinowski, G., Kamiński, M., & Wawer, D., *Trans3D: a free tool for dynamical visualization of EEG activity transmission in the brain*, Computers in Biology and Medicine, 51, 214-222. 2014.

[C4] Blinowska K., Kamiński M., Baccala, L., Sameshima K., Blinowski G., E*stimation of Effective Connectivity from Electrophysiological Time Series* (A Special Sessions Tutorial), Proceedings - Type II, Web Inteligence Congress, 11-14 August 2014, Warsaw, Poland

Słownik skrótów pojawiających się w rozdziałach od 4.5 do 5

ASN.1 – Abstract Syntax Notation One

BER – Basic Encoding Rules (BER)

CMS – Certificate Management System

ESMTP – Extended Simple Mail Protocol

IMAP – Internet Message Access Protocol (jeden z pomocniczych protokołów w systamach email)

LDAP – Lightweight Directory Access Protocol

PGP – Pretty Good Privacy

PKI – Public Key Infrastructure

POP – Post Office Protocol (jeden z pomocniczych protokołów w systamach email)

S/MIME – Secure Multipurpose Internet Mail Extensions

XML-RPC – remote procedure call with XML

EEG – Elektroencefalografia

ERP – Event-related potential (potencjał wywołany - odmiana EEG).

LFP – local field potential (potencjał międzykomórkowy na poziome neuronów)

6. Informacja o osiągnięciach dydaktycznych, organizacyjnych oraz popularyzujących naukę lub sztukę.

6.1 Osiągnięcia dydaktyczne

- Samodzielnie opracowałem wykład oraz zadania projektowe dla przedmiotu: ***Programowanie Sieciowe (PSI)***. Wspólnie z zespołem pracowników laboratorium Instytutu Informatyki opracowaliśmy i wdrożyliśmy też środowisko kontenerowe, w którym realizowane są zadania projektowe. Współtworzyłem, a następnie samodzielnie modyfikowałem sylabus przedmiotu (2019 – 2024).

- Samodzielnie opracowałem wykład, laboratorium oraz zadania projektowe dla przedmiotu: ***Techniki Internetowe (TIN)***. W trakcie realizacji tego przedmiotu wielokrotnie aktualizowałem zakres zgodnie z rozwojem standardów i technologii, wprowadzając m.in. takie zagadnienia jak: protokół IPv6 i HTTP 2. (2003 – 2019)

- Prowadzę obieralny przedmiot ***Unix Architektura i Programowanie (UXP1A)*** (wykład oraz projekt). W wieloletnim okresie prowadzenia ww. przedmiotu przekształciłem jego formułę ze zorientowanego na systemy komercyjne UNIX (bazujące na wersji UNIX SVR4) na warianty darmowe: Linux oraz BSD, stale aktualizując zakres zgodnie z tendencjami rozwoju tego systemu - np. ostatnio przez rozszerzenie tematyki zajęć o mechanizmy konteneryzacji. (2001 – 2024)

Przedmioty (ćwiczenia, projekty, laboratoria oraz wykłady) prowadzone od 2001 r.:

- Sieci Komputerowe (SKOM), 2003
- Systemy Operacyjne (SOI), 2003
- Analiza Algorytmów (AAL), 2013 - 2020Z (z przerwami)
- Podstawy Sztucznej Inteligencji (PSZT), a następnie Wstęp do Sztucznej Inteligencji (WSI), 2018 - 2019L
- Techniki Internetowe (TIN), 2003 - 2021Z (wykład, projekt)
- Programowanie Sieciowe (PSI), 2021Z - 2023Z (wykład, laboratorium, projekt)
- Unix Programowanie i Architektura (UXP1A), 2001 - 2023 (wykład, projekt)

Opieka naukowa nad studentami

Od 2001 (po uzyskaniu doktoratu) byłem promotorem 20 prac dyplomowych inżynierskich i 24 magisterskich (łącznie, od początku zatrudnienia na Politechnice Warszawskiej, 51 wypromowanych prac). Aktualnie pod moją opieką jest 3 dyplomantów: 2 na studiach inżynierskich i 1 na studiach magisterskich. Tematyka prowadzonych prac dyplomowych związana jest ściśle z prowadzonymi badaniami. Poniżej znajduje się lista artykułów, w których zaznaczono współautorów będących moimi studentami:

— Blinowski, G., **Ciechańska, K**., *KCMail - wydajny filtr protokołu SMTP*; Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne 7/2013 ISSN 1230-3496. 2013.

— Blinowski, G., **Pieczerak, T**., *Układ Raspberry Pi jako uniwersalna platforma mikro-appliance do zastosowań sieciowych i bezpieczeństwa*. Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne, nr 7/2014.

— Blinowski, G., **Kmieciak, A**., *Modelling and evaluation of a multi-tag LED-ID platform*. Proc. Federated Conference on Computer Science and Information Systems (FEDCSIS), Gdańsk, Poland, 11 - 14 September, 2016.

— Blinowski, G.; **Mościcki, A**., *Comparing Gausian and exact models of malicious interference in VLC systems*, International Journal of Electronics and Telecommunications, Vol. 65. 2019.

— Blinowski, G., **Piotrowski, P**., *CVE based classification of vulnerable IoT systems*; International Conference on Dependability and Complex Systems; pp. 82-93, Springer. 2020.

— Blinowski, G. J., **Piotrowski, P., Wiśniewski, M**. (2021). *Comparing Support Vector Machine and Neural Network Classifiers of CVE Vulnerabilities*; Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021), pages 734-740, ISBN: 978-989-758-524-1

— Blinowski, G. J., **Szaknis, M**. (2024). *Fuzzing Trusted Environments with Rust*; Computers & Security (2024), _____

6.2 Nagrody

- W **2013** otrzymałem Nagrodę indywidualną II stopnia JM Rektora PW za osiągnięcia dydaktyczne w roku 2012 Nagroda za wydaną w 2012 roku przez wydawnictwo BTC książkę pt. "*Systemy poczty elektronicznej. Standardy, architektura, bezpieczeństwo*".

- W **2014** wraz z Krzysztofem Cabajem (WEiTI/II), Piotrem Gawrysiakiem (WEiTI/II), Waldemarem Grabskim (WEiTI/II), Rajmundem Kożuszkiem (WEiTI/II), Dominikiem Ryżko (WEiTI/II) i Łukaszem Skoniecznym (WEiTI/II) otrzymałem Nagrodę Zespołową I stopnia JM Rektora PW za osiągnięcia organizacyjne w latach 2012 - 2013 za przygotowanie merytoryczne Ogólnopolskiej Olimpiady Wiedzy o Internecie Net Masters Cup.

6.3 Inna działalność edukacyjna i popularyzatorska

Kierowałem zespołem odpowiedzialnym za przygotowanie **dystrybucji systemu Linux przeznaczonego do celów edukacyjnych**. Opracowana przez nasz zespół dystrybucja o nazwie „*NELinux*" (Linux Nowej Ery) dołączona została **do podręcznika informatyki przeznaczonego dla klas 1-3 gimnazjum, opracowanego przez wydawnictwo Nowa Era**. Autorem podręcznika był Piotr Jerzy Durka, koordynatorem projektu Marek Faber (Wydawnictwo Nowa Era i Instytut Systemów Elektronicznych Politechniki Warszawskiej). Opracowana dystrybucja charakteryzowała się: wysoką przenośnością, dostosowaniem do parametrów sprzętowych komputera użytkownika (za szczególnym uwzględnieniem komputerów o niewielkiej wydajności); zawierała też szereg starannie dobranych i odpowiednio skonfigurowanych programów edukacyjnych. (2005 – 2007)

Wraz z zespołem pracowników Instytutu Informatyki wziąłem udział w przygotowaniu merytorycznym **Ogólnopolskiej Olimpiady Wiedzy o Internecie Net Masters Cup**, realizując zadania Politechniki Warszawskiej jako partnera merytorycznego Olimpiady. Net Masters Cup był wówczas największym w Polsce i jednym z większych w Europie konkursów wiedzy o Internecie i technologiach informatycznych, skierowanym do młodzieży ponadgimnazjalnej oraz nauczycieli informatyki. Za ww. prace w 2014 otrzymałem Nagrodę zespołową I stopnia JM Rektora PW. (2012 – 2013)

Pod auspicjami polskiego oddziału organizacji ISSA (Information Systems Security Association) **współuczestniczyłem w opracowaniu materiałów informacyjnych do kampanii „Cyberbezpieczeństwo”**, które ukazały się na łamach dziennika „Rzeczpospolita” oraz dedykowanego portalu informacyjnego „Poradnik biznesu”. Kampania była skierowana głównie do sektora B2B, a jej celem było edukowanie i informowanie przedsiębiorców w zakresie szeroko pojętej tematyki zabezpieczeń infrastruktury sieciowej. (2015)

6.4 Członkostwo i działalność w stowarzyszeniach i organizacjach

J**estem członkiem zwykłym IEEE** (Institute of Electrical and Electronics Engineers). (Od 2017)

Posiadam certyfikat CISSP (Certified Information Systems Security Professional) przyznawany przez organizację non-profit ISC2 (International Information System Security Certification Consortium). CISSP jest certyfikatem eksperckim w dziedzinie bezpieczeństwa informacji, który spełnia wymogi standardu ISO/IEC 17024:2003. Przyznanie certyfikatu warunkowane jest zdaniem egzaminu obejmującego wiedzę z zakresu dziesięciu tzw. „domen” bezpieczeństwa systemów i informacji. Utrzymanie certyfikatu jest warunkowane corocznym audytem potwierdzającym kompetencje przeprowadzanym przez ISC2. (Od 2014).

J**estem członkiem polskiego oddziału ISSA** (Information Systems Security Association) - międzynarodowej organizacji zawodowej non-profit zrzeszającej specjalistów i praktyków z zakresu bezpieczeństwa informacji. (Od 2015)

7. Oprócz kwestii wymienionych w pkt. 1-6, wnioskodawca może podać inne informacje, ważne z jego punktu widzenia, dotyczące jego kariery zawodowej.
