POLITECHNIKA GDAŃSKA

3 czerwca 2020

Katedra Teleinformatyki
Tematy prac dyplomowych magisterskich dla kierunku INFORMATYKA
rok akademicki 2020/2021

1. Analiza bezpieczeństwa i prywatności usług autokonfiguracji sieci IP;
2. Analiza bezpieczeństwa rozszerzeń funkcjonalnych infrastruktury klucza publicznego (PKI);
3. Analiza mechanizmów wykrywania pętli w sieciach Ethernet ;
4. Analiza oraz porównanie rozwiązań zbierania i przetwarzania danych dotyczących urządzeń sieciowych;
5. Analiza porównawcza algorytmów kryptografii post-kwantowej;
6. Analiza porównawcza metod filtracji ruchu szyfrowanego HTTPS w sieci firmowej;
7. Badania mechanizmu reputacyjnego RISC2WIN dla komunikacji kooperatywnej 5G;
8. Implementacja zgodnych motywacyjnie systemów reputacyjnych w wybranych środowiskach teleinformatycznych;
9. Koncepcja i implementacja protokołu MQTT dla sieci DTN o nieciągłej i sporadycznej łączności;
10. Mechanizm budowy zaufania dla ochrony przed atakami metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług;
11. Ocena implementacji systemów monitorowania strumieniowania multimediów dla rozgłośni radiowych;
12. Ocena miar sprawiedliwości indywidualnej i systemowej;
13. Ocena możliwości manipulacji w systemach reputacyjnych stosowanych w wybranych środowiskach teleinformatycznych;
14. Ocena możliwości nadużyć i przeciwdziałania im w rozwiązaniach uprawomocnionego podsłuchiwania;
15. Ocena możliwości realizacji sieci pierścieniowych z mechanizmami sprawiedliwości;
16. Ocena możliwości wykonania filtra ukrytych kanałów w ruchu sieciowym;
17. Ocena możliwości wykorzystania detekcji oraz inspekcji ruchu szyfrowanego do zwalczania złośliwego oprogramowania;
18. Ocena możliwości wykorzystanie koncepcji Internetu Rzeczy w systemach obsługi wołań w niebezpieczeństwie;
19. Ocena wpływu parametrów QoE na współczynnik churn;
20. Porównanie rozwiązań typu open-source do monitorowania klastra Kubernetes w środowisku produkcyjnym;
21. Projekt niezawodnego systemu sieciowego odpornego na umyślne działania niszczące;
22. Przegląd i analiza mechanizmów tworzenia wirtualnych struktur sieciowych w systemie OpenStack;
23. Przegląd i analiza popularnych środowisk orkiestracji aplikacji skonteneryzowanych;
24. Przegląd narzędzi do zarządzania konfiguracją i realizacji usług Infrastructure as a Code w środowisku chmur obliczeniowych;
25. Realizacja metody niezawodnej transmisji informacji w sieci FSO (Free Space Optical) odpornej na zakłócenia spowodowane czynnikami pogodowymi;
26. Realizacja metody niezawodnej transmisji informacji w zastosowaniach sieci z transmisją odporną na opóźnienia;
27. Realizacja metody szybkiego odtworzenia transmisji po awarii w sieciach IP;

28. Realizacja metody ochrony transmisji w sieci teleinformatycznej przed awarią masową uwarunkowaną umyślnym działaniem niszczącym;
29. Strategie obrony sieci bezprzewodowych o topologii wieloskokowej przed inteligentnymi atakami metodą podmiany klasy ruchu;
30. Zastosowanie uczenia maszynowego do projektowania strategii ataku metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług;
31. Analiza mechanizmów zapewniania skalowalności sieci Ethetnet.

Temat 1	Analiza bezpieczeństwa i prywatności usług autokonfiguracji sieci IP.
Temat w języku angielskim	Analysis of security and privacy of IP network auto-configuration services.
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Cel pracy	Celem pracy jest analiza atrybutów bezpieczeństwa, niezawodności i prywatności usług autokonfiguracji sieci IP oraz opracowanie projektu mechanizmu zwiększającego poziom wybranego atrybutu. Temat uzgodniony ze studentem 165498
Zadania	Przegląd stanu obecnego usług autokonfiguracji sieci IP. Analiza stanu mechanizmów bezpieczeństwa, niezawodności i prywatności. Propozycje dobrych praktyk w zakresie istniejących mechanizmów. Projekt i testowa implementacja własnej propozycji nowego mechanizmu zwiększającego stopień bezpieczeństwa, albo niezawodności, albo prywatności wybranej usługi.
Literatura	Standardy RFC dotyczące autokonfiguracji sieci m. in. RFC2131, RFC3315, RFC4862, RFC1035, RFC6762, RFC6763 wraz z aktualizacjami i rozszerzeniami. A. S. Tanenbaum, D. J. Wetherall, Computer Networks (5th Edition), Pearson Education Inc., 2011

Temat 2	Analiza bezpieczeństwa rozszerzeń funkcjonalnych infrastruktury klucza publicznego (PKI)
Temat w języku angielskim	Security study on Public Key Infrastructure (PKI) functional extensions
Opiekun pracy	dr inż. Tomasz Gierszewski

Konsultant pracy	
Cel pracy	Infrastruktura klucza publicznego stanowi najbardziej dojrzałe rozwiązanie pozwalające zabezpieczać komunikację we współczesnych sieciach komputerowych. Nastręcza jednak trudności pod względem zarządzania, począwszy do dystrybucji kluczy publicznych podmiotów, pomiędzy którymi ma zachodzić komunikacja, na zarządzaniu listą zaufanych urzędów certyfikacji (CA) kończąc. Na przestrzeni lat opracowano szereg koncepcji uzupełnienia funkcjonalnego niedomagań PKI – od projektu Perspectives, poprzez protokoł HSTS i HPKP, na rozwiązaniu Certificate Transparency kończąc. Nie jest to kompletna lista. Celem pracy jest ocena bezpieczeństwa, niejednokrotnie opracowywanych pod presją czasu, rozwiązań.
Zadania	W ramach pracy przewiduje się realizację następujących zadań: 1. Przegląd rozwiązań funkcjonalnych uzupełniających infrastrukturę klucza publicznego 2. Analiza porównawcza rozwiązań – podjęcie próby ich systematyzacji 3. Analiza bezpieczeństwa scharakteryzowanych mechanizmów 4. Propozycja środków poprawiających bezpieczeństwo – proceduralnych lub technicznych
Literatura	1. Jøsang, A.: PKI trust models. In Theory and Practice of Cryptography Solutions for Secure Information Systems (pp. 279-301). IGI Global, 2013 2. Laurie, B.: Certificate transparency. Communications of the ACM, 57(10), 40-46, 2014 3. de los Santos, S., Torrano, C., Rubio, Y., & Brezo, F.: Implementation state of HSTS and HPKP in both browsers and servers. In International Conference on Cryptology and Network Security (pp. 192-207). Springer, Cham, 2016 4. Helme S.: I'm giving up on HPKP, online: https://scotthelme.co.uk/im-giving-up-on-hpkp/ 2017

Temat 3	Analiza mechanizmów wykrywania pętli w sieciach Ethernet
Temat w języku angielskim	Analysis of loop detection mechanisms ii Ethernet networks
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem pracy jest analiza mechanizmów zapewniania bezpetlowej pracy sieci Ethernet
Zadania	1. Przegląd mechanizmów zapewniania bezpętlowej pracy sieci Ethernet – szczegółowy opis algorytmów drzewa opinającego, SPB, TRILL 2. Zaproponowanie modyfikacji wybranego mechanizmu zapewniania bezpętlowej pracy 3. Implementacja zaproponowanej modyfikacji (albo w systemie rzeczywistym alblbo w systemie zwirtualizowanym albo w symulatorze)

	4. Porównanie klasycznych i zmodyfikowanych rozwiązań
Literatura	1. Nowicki K., Uhl T.: Monitorowanie i bezpieczeństwo sieci komputerowych. Szczecin: Wydawnictwo Naukowe Akademii Morskiej w Szczecinie, 2016.148 s. ISBN 970−83−64434−08−2 2. Nowicki K., Uhl T.: Ethernet end-to-end. Eine universelle Netzwerktechnologie. Aachen: Shaker Verlag, 2008. 225 s. ISBN 978-3-8322-7140-4 3. Nowicki K.: Ethernet - sieci, mechanizmy. Gdańsk: INFOTECH, 2006.152 s. ISBN 83-921711-2-8 4. Nowicki K., Malinowski A..: Topology Discovery of Hierarchical Ethernet LANs without SNMP support, W: The 41st Annual Conference of the IEEE Industrial Electronics Society, 2015, IEEE Industrial Electronics Society 5. Nowicki K., Ostrowski A., Poźniak A., Wrzesiński Ł.: Wykorzystanie sprzętu komputerowego klasy SOHO do modelowania złożonych rozwiązań sieciowych// STUDIA INFORMATICA. SYSTEMS AND INFORMATION TECHNOLOGY. SYSTEMY I TECHNOLOGIE INFORMACYJNE. -Vol. 32., nr. Nr 3A (98) (2011), s.55-66 6. Allan D., Bragg N.: 802.1aq Shortest Path bridging. Design and Evolution, Willey, IEEE, 2012 7. https://datatracker.ietf.org/wg/trill/charter/

Temat 4	Analiza oraz porównanie rozwiązań zbierania i przetwarzania danych dotyczących urządzeń sieciowych
Temat w języku angielskim	Analysis and comparison of network device monitoring solutions
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	Zbieranie danych i odpowiednia ich obróbka jest ważnym elementem rozwiązań pomagających zapewnić stabilność i niezawodność sieci pozwalającym na szybką reakcję w przypadku niestandardowych zachowań lub awarii. Celem pracy jest dokonanie przeglądu i analizy wykorzystywanych rozwiązań tego typu, określenie głównych kierunków ich rozwoju, a także funkcjonalności uznawanych za kluczowe oraz sposobów ich realizacji. W kontekście uzyskanych wyników zostanie też przeprowadzony przegląd aktualnych metod zbierania danych dotyczących pracy urządzeń sieciowych w CI TASK. Wyniki badań mają pozwolić na znalezienie rozwiązań odpowiadających dzisiejszym standardom przy minimalizacji zużywanych zasobów sprzętowych.
Zadania	• Przegląd i analiza rozwiązań monitorowania urządzeń sieciowych dostępnych na rynku, włączając dedykowane rozwiązania udostępniane przez dostawców sprzętu sieciowego. • Przegląd aktualnych rozwiązań stosowanych przez CI TASK • Wdrożenie wybranych rozwiązań w środowisku laboratoryjnym.
Literatura	• Monitoring i bezpieczeństwo sieci / Chris Fry, Martin Nystrom / O'Reilly 2010 • Wykrywaj i reaguj. Praktyczny monitoring sieci dla administratorów / Richard Bejtlich / Helion 2014 • Dokumentacja CI TASK

Temat 5	Analiza porównawcza algorytmów kryptografii post-kwantowej

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Temat w języku angielskim	Comparative analysis of post-quantum cryptography algorithms
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Crypto-agility jest na chwilę obecną rekomendowanym sposobem przygotowania zabezpieczeń kryptograficznych technikę kwantową, która może zagrozić aksjomatom stosowanych obecnie algorytmów. Oznacza to, że projektowane aktualnie zabezpieczenia powinny wyróżniać się zwinnością, w szczególności pod względem wymiany materiału kryptograficznego, ale także zastosowanych algorytmów. Ponieważ nie we wszystkich środowiskach taka zwinność jest łatwa do osiągnięcia, już teraz opracowywane są liczne algorytmy, których złożoność z jednej strony będzie stanowiła barierę dla komputerów kwantowych, z drugiej – nałoży ciężar obliczeniowy możliwy do osiągnięcia przez współczesne nie-kwantowe systemy informatyczne. Celem pracy jest usystematyzowanie aktualnych dokonań na tym polu, ze szczególnym uwzględnieniem istniejących i powstających implementacji możliwych do wykorzystania w niedalekiej przyszłości.
Zadania	W ramach pracy przewiduje się realizację następujących zadań: 1. Krytyka stosowanych algorytmów w świetle techniki kwantowej 2. Przegląd i charakterystyka klas problemów matematycznych, wokół których skupiają się algorytmy kryptografii post-kwantowej 3. Przegląd i systematyka algorytmów kryptografii post-kwantowej ze szczególnym uwzględnieniem konkursu PQCrypto organizowanego przez NIST 4. Przegląd stanu implementacji i popularyzacji algorytmów w powszechnie stosowanych bibliotekach kryptograficznych 5. Analiza porównawcza wybranych algorytmów kryptografii post-kwantowej
Literatura	1. Kuznetsov, A., Kiian, A., Lutsenko, M., Chepurko, I., Kavun, S.: Code-based cryptosystems from NIST PQC. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 282-287). IEEE, 2018 2. Banerjee, T., Hasan, M. A.: Energy consumption of candidate algorithms for NIST PQC standards. Technical report, Centre for Applied Cryptographic Research (CACR) at the University of Waterloo http://cacr. uwaterloo. ca/, Accessed 26 June, 2018 3. Strona projektu PQC (Post-Quantum Crypto) https://csrc.nist.gov/Projects/post-quantum-cryptography

Temat 6	Analiza porównawcza metod filtracji ruchu szyfrowanego HTTPS w sieci firmowej.
Temat w języku angielskim	Comparative analysis of HTTPS encrypted traffic filtering methods in a corporate network.
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Cel pracy	Celem pracy jest wykonanie wielokryterialnej analizy porównawczej metod filtracji ruchu szyfrowanego HTTPS. Temat uzgodniony ze studentem 165700.

Zadania	Przegląd stanu sztuki. Analiza porównawcza najpopularniejszych rozwiązań programowych i sprzętowych. Demonstrator wybranych technologii.
Literatura	Dokumetacja mechanizmu netfilter w jądrze systemu Linux. Dokumentacja oprogramowania pfSense i Squid. Dokumentacja urządzeń zabezpieczeających sieci firm Cisco, Juniper i Fortinet. A. S. Tanenbaum, D. J. Wetherall, Computer Networks (5th Edition), Pearson Education Inc., 2011

Temat 7	**Badania mechanizmu reputacyjnego RISC2WIN dla komunikacji kooperatywnej 5G**
Temat w języku angielskim	**Study of the RISC2WIN reputation mechanism for cooperative 5G communications**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Cel pracy	Celem pracy jest przebadanie mechanizmu budowania reputacji jako gwaranta uczciwego różnicowania jakości usług (QoS) przez stacje pośredniczącą w 2-skokowej sieci bezprzewodowej.
Zadania	1. Specyfikacja i implementacja mechanizmu w narzędziu symulacyjnym 2. Symulacja i analiza strategiczna gry pomiędzy stacją pośredniczącą i końcową 3. Określenie optymalnych przebiegów trajektorii bieżących wartości reputacji dla różnych scenariuszy ruchowych 4. Wykonanie demonstratora zasilanego sztucznym źródłem ruchu webowego i VoIP
Literatura	1. S. Szott and J. Konorski, "Selfish attacks in two-hop IEEE 802.11 relay networks: impact and countermeasures," IEEE Wireless Comm. Letters, DOI: 10.1109/LWC.2018.2809726. 2. A. Garcia-Saavedra, B. Rengarajan, P. Serrano, D. Camps-Mur, and X. Costa-Pérez, "SOLOR: self-optimizing WLANs with legacy-compatible opportunistic relays," IEEE/ACM Trans. on Networking, vol. 23, no. 4, pp. 1202-1215, Aug. 2015. 3. N. Zhao, Y. C. Liang, and Y. Pei, "Dynamic contract design for cooperative wireless networks," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 4. B. Jedari, F. Xia and Z. Ning, "A Survey on Human-Centric Communications in Non-Cooperative Wireless Relay Networks," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 914-944, 2018.

	5. A. Malik, J. Qadir, B. Ahmad, K.-L. Alvin Yau, and U. Ullah, "QoS in IEEE 802.11-based wireless networks: a contemporary review," Journal of Network and Computer Applications, vol. 55, pp. 24-46, 2015. 6. inne materiały źródłowe dostępne u opiekuna

Temat 8	Implementacja zgodnych motywacyjnie systemów reputacyjnych w wybranych środowiskach teleinformatycznych
Temat w języku angielskim	**Implementation of incentive compatible reputation systems in selected computer communication settings**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Cel pracy	Celem pracy jest przebadanie zasad i protokołów współpracy autonomicznych agentów racjonalnych zapewniających prawdomówność raportowania o zaobserwowanych zachowaniach innych agentów.
Zadania	1. Specyfikacja protokołów współpracy agentów. 2. Budowa modelu symulacyjnego w środowisku sieci bezprzewodowych oraz społecznościowych 3. Ocena wpływu rzeczywistych parametrów środowiska na skuteczność wybranych protokołów współpracy agentów
Literatura	1. Jurca R., B. Faltings, *An incentive compatible reputation mechanism*, Proc. 2nd AAMAS, 2003 2. Jurca R., B. Faltings, *Collusion-resistant, incentive-compatible feedback payments*, Proc. 8th ACM Conf. on Electronic Commerce, 2007 3. Miller N., P. Resnick, R. Zeckhauser, *Eliciting informative feedback: the peer-prediction method*, *Management Science* vol. 51, 2005 4. J. Konorski, *Reputacja i zaufanie w systemach teleinformatycznych z podmiotami anonimowymi - podejście dynamiczne*, Przegląd Telekomunikacyjny, t. LXXXIX, 2016

Temat 9	Koncepcja i implementacja protokołu MQTT dla sieci DTN o nieciągłej i sporadycznej łączności.
Temat w języku angielskim	The concept and implementation of the MQTT protocol for DTN networks with discontinuous and sporadic connectivity.
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Cel pracy	Celem pracy jest analiza możliwości rozszerzenia protokołu MQTT do zarządzania pracą urządzeń mobilnych w sieciach DTN o nieciągłej sporadycznej łączności wraz z implementacją demonstratora.
Zadania	Przegląd stanu sztuki.

	Analiza problemów w sieciach DTN. Opracowanie koncepcji i projektu rozwiązania. Implementacja demostratora. Testy i analiza wniosków.
Literatura	K. Fall, "A delay-tolerant network architecture for challenged internets" Computer Communications Review, New York 2003 Dokumentacja MQTT http://mqtt.org A. S. Tanenbaum, D. J. Wetherall, Computer Networks (5th Edition), Pearson Education Inc., 2011

Temat 10	Mechanizm budowy zaufania dla ochrony przed atakami metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług
Temat w języku angielskim	A trust building mechanism to defend against Fake VIP attacks in computer communication systems supporting QoS differentiation
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Cel pracy	W systemach teleinformatycznych wspierających różnicowanie jakości usług (QoS) atak metodą fałszywego VIPa jest odmianą niewykrywalnej uzurpacji uprawnień. W obliczu żądania usług mogącego być częścią takiego ataku agent IDS ma do wyboru uruchomienie kosztownej procedury weryfikacji sygnatury ataku (np. DPI - *deep packet inspection*), bądź okazanie zaufania i przydział żądanego poziomu QoS. IDS dąży do jednoczesnego ograniczenia kosztu DPI oraz częstości przydziału nienależnie wysokiego poziomu QoS, zaś atakujący intruz - do możliwie częstego przydziału nienależnie wysokiego poziomu QoS. Celem pracy jest eksperymentalne zbadanie skuteczności mechanizmu zaufania w IDS dyktującego decyzje o uruchomieniu DPI dla kolejnych żądań usług
Zadania	1. Opis mechanizmu ataku metodą fałszywego VIPa w różnych środowiskach sieciowych 2. Analiza możliwych mechanizmów obronnych oraz ich penetracji przez racjonalnego intruza ze zdolnością uczenia się 3. Sformułowanie modelu agenta IDS, intruza i systemu komunikacyjnego oraz pozyskanie zbiorów danych wejściowych do eksperymentów 4. Analiza skuteczności systemu budowy zaufania w warunkach stabilnej generacji żądań usług i pracy systemu komunikacyjnego.
Literatura	1. Y. L. Sun, Y. Liu, *Security of online reputation systems: The evolution of attacks and defenses*, IEEE Signal Proc. Mag., vol. 29, 201

POLITECHNIKA GDAŃSKA

	2. Po-Ching Lin et al., *Using String Matching for Deep Packet Inspection*, Computer, vol. 41, 2008 3. Patcha, Jung-Min Park, *A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks*, Int. J. of Network Security vol. 2, 2006. 4. T. Grandison and M. Sloman, *A survey of trust in internet applications*, IEEE Comm. Surveys & Tutorials, vol. 3, 2000. 5. P. L. Bartlett, *Online Prediction*. 2015, stat.berkeley.edu/~bartlett/papers/b-ol-16.pdf 6 Y. Freund et al., *Efficient Algorithms for Learning to Play Repeated Games Against Computationally Bounded Adversaries*, Proc. 36th Annual Symp. Foundations of Computer Science, 1995.

Temat 11	Ocena implementacji systemów monitorowania strumieniowania multimediów dla rozgłośni radiowych
Temat w języku angielskim	Assessment of the implementation of multimedia streaming monitoring systems for radio stations
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	mgr inż. Łukasz Wiszniewski
Cel pracy	Każda rozgłośnia radiowa strumieniująca swoje programy potrzebuje informacji kto (co najmniej nr IP), kiedy, jak długo, gdzie, jak, … wykorzystuje ich strumienie. Taką rozgłośnią jest, w szczególności, Radio Gdańsk, które wykorzystuje zasoby techniczne TASK. Celami pracy są 1. dokonanie przeglądu istniejących systemów monitorowania strumieniowania wykorzystywanych przez firmy multimedialne, w szczególności radiowe, ich porównanie i skonfrontowanie z wymaganiami polskiej, regionalnej rozgłośni. 2. zaproponowanie modyfikacji jednego z rozwiązań dostępnych na rynku uwzględniającej z jednej strony specyfikę rozgłośni (Radio Gdańsk), a z drugiej strony operatora (TASK). 3. ocena swojej propozycji z wybranym systemem dostępnym na rynku
Zadania	1. Przegląd istniejących rozwiązań systemów monitorowania strumieniowania 2. Propozycja systemu umożliwiającego analizę zachowania użytkownika odbierającego strumień multimedialny w szczególności jego • geolokalizację, • czas odbierania strumienia, • możliwość korelacji danych o użytkowniku z danymi uzyskanymi od nadawcy 3. Określenie kryteriów porównawczych systemów monitorowania

	4. Analiza porównawcza wybranego systemu monitorowania z zaproponowanym systemem
Literatura	1. Dokumentacja systemów strumieniujących dane (np. Wowza) 2. Dokumentacja informacji o ruchu sieciowym w CI TASK 3. Dokumentacja wybranych systemów monitorowania 4. zasoby internetu

Temat 12	Ocena miar sprawiedliwości indywidualnej i systemowej
Temat w języku angielskim	Assessment of individual and system fairness
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem pracy jest ocean uzytecznosci miar sprawiedliwosci przydziału zasobów, w szczególnosci do oceny sprawiedliwosci indywidualnej
Zadania	1. Zapoznanie z problemami zapewniania sprawiedliwosci w sieciach komputerowych, w szczególnosci miarami sprawiedliwosci 2. Wybór mechanizmów zapewniania sprawieliwości w sieciach 3. Przegląd dostępnych środowisk symulacyjnych 4. Wybór srodowiska symulacyjnego 5. Zaprojektowanie i implemetacja mechanizmów sprawieliwości w środowisku symulacyjnym i ocena ich jakości pod kątem sprawiedliwości indywidualnej i systemowej Podsumowanie – próba odpowiedzi na pytanie "Jaka ze znanych miar sprawiedliwosci najlepiej nadaje sie do oceny systemów, w których pominięcie, przydzielenie nieproporcjonalnie małych zasobów jest niedopuszczalne.
Literatura	1. Antkiewicz J., Sznyter B.: Projekt i implementacja symulatora sieci pierścieniowej, praca inżynierska WETI PG 2018 2. Nowicki K., Malinowski A., Sikorski M..: More Just Measure of Fairness for Sharing Network Resources, W: 23rd International Conference on Computer Networks (CN), 2016, Springer 3. Shi H., Prasad V., Onur E., Niemegeers I.G.M.M.: Fairness in Wireless Networks - Issues, Measures and Challenges, *IEEE Communications Surveys and Tutorials*, pp. 5-24, 2013, PDF. 4. Zasoby Internetu

Temat 13	**Ocena możliwości manipulacji w systemach reputacyjnych stosowanych w wybranych środowiskach teleinformatycznych**
Temat w języku angielskim	**Feasibility of a reputation system manipulation in selected computer communication settings**
Opiekun pracy	dr hab. inż. Jerzy Konorski

Konsultant pracy	
Cel pracy	Celem pracy jest przebadanie zasad i protokołów współpracy autonomicznych agentów racjonalnych opartych na generowaniu danych reputacyjnych ze szczególnym uwzględnieniem możliwości odwrócenia hierarchii uczciwości agentów.
Zadania	1. Specyfikacja protokołów zbierania przetwarzania danych reputacyjnych. 2. Budowa modelu symulacyjnego agentów o zróżnicowanym stopniu uczciwości w wybranym środowisku teleinformatycznym 3. Ocena wpływu rzeczywistych parametrów środowiska na skuteczność manipulacji w systemie reputacyjnym.
Literatura	1. Y. L. Sun, Y. Liu, *Security of online reputation systems: The evolution of attacks and defenses*, IEEE Signal Proc. Mag., vol. 29, 2012 2. Miller N., P. Resnick, R. Zeckhauser, *Eliciting informative feedback: the peer-prediction method*, *Management Science* vol. 51, 2005 3. J. Konorski, *Reputacja i zaufanie w systemach teleinformatycznych z podmiotami anonimowymi - podejście dynamiczne*, Przegląd Telekomunikacyjny, t. LXXXIX, 2016

Temat 14	Ocena możliwości nadużyć i przeciwdziałania im w rozwiązaniach uprawomocnionego podsłuchiwania
Temat w języku angielskim	Feasibility study on lawful interception abuse and its prevention
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Uprawomocnione podsłuchiwanie (ang. Lawful Interception) jest mechanizmem pozwalającym organom władzy wykonawczej podsłuchiwać między innymi rozmowy telefoniczne. W przypadku szyfrowania ruchu istnieje szereg praktyk, które pozwalają sobie radzić z taką inspekcją: ominięcie szyfrowania, składowanie kluczy sesyjnych razem z zapisem, pośredniczenie w negocjowaniu kluczy sesyjnych. Takie podsłuchiwanie w założeniu powinno być realizowane w stanie wyższej konieczności. Celem pracy jest ocena możliwości nadużywania, jak również detekcji nadużyć mechanizmów uprawomocnionego podsłuchiwania.
Zadania	W ramach pracy przewiduje się realizację następujących zadań: 1. Systematyka technik uprawomocnionego podsłuchiwania ruchu szyfrowanego 2. Przegląd narzędzi inspekcji ruchu SSL/TLS – zarówno Open Source, jak i komercyjnych 3. Ocena możliwości detekcji inspekcji po stronie nadawcy i odbiorcy 4. Projekt i implementacja dowodu poprawności rozumowania dla popularnych rozwiązań strony klienta i/lub serwera

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Literatura	1. O'Neill, M., Ruoti, S., Seamons, K., Zappala, D.: TLS Inspection: How Often and Who Cares?. IEEE Internet Computing, 21(3), 22-29, 2017 2. dokumentacja rozwiązania SSLH 3. dokumentacja komercyjnych rozwiązań NGFW pozwalających wykonać inspekcję ruchu szyfrowanego

Temat 15	Ocena możliwości realizacji sieci pierścieniowych z mechanizmami sprawiedliwości
Temat w języku angielskim	Assessment of the feasibility of ring networks with fairness mechanisms
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Ocena sprawiedliwości w sieciach pierścieniowych
Zadania	1. Przegląd rozwiązań sieci pierścieniowych (w tym teleinformatycznych, telekomunikacyjnych i przemysłowych) 2. Przegląd i porównanie mechanizmów sprawiedliwości realizowanych w sieciach komputerowych 3. Propozycja modyfikacji wybranego mechanizmu sprawiedliwości umożliwiającego jego wykorzystanie w sieci pierscieniowej 4. Ocena jakosci zaproponowanego systemu (symulacyjna albo analityczna)
Literatura	[1] F. Davik, A. Kvalbein, S. Gjessing, Improvement of resilient packet ring fairness, IEEE GLOBECOM, pp. 1-17 (2005)[2] D. Nace M. Pioro: "Max-min fairness and its applications to routing and load-balancing in communication networks: a tutorial," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 5-17 (2008) [3] A. Ahmad, M.T. Beg, S.N. Ahmad: "Fairness Issues and Measures in Wireless Networks: A Survey," *IOSR Journal of Electronics and Communication Engineering* (IOSR-JECE), vol. 11, no. 6, pp. 20-24, 2016. [4] K. Nowicki, A. Malinowski, M. Sikorski: "More Just Measure of Fairness for Sharing Network Resources," Proc. 23rd International Conference on Computer Networks*, Communications in Computer and Information Science*, Springer, vol. 608, pp. 52-58, 2016. [5] T. Hoßfeld, L. Skorin-Kapov, P.E. Heegaard, M. Varela: A new QoE fairness index for QoE management, *Quality and User Experience*, February 2018, doi.org/10.1007/s41233-018-0017-x [6] Ryoo, J.-d., et al. (2008). Ethernet ring protection for carrier Ethernet networks. *IEEE Communications Magazine, 46*(9), 136–143. [7] Bistouni, F., & Jahanshahi, M. (2017). Reliability analysis of Ethernet ring mesh networks. *IEEE Transactions on Reliability, 66*(4), 1238–1252. Zasoby Internetu

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Temat 16	Ocena możliwości wykonania filtra ukrytych kanałów w ruchu sieciowym
Temat w języku angielskim	Feasibility study on filtering hidden channels in network traffic
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	
Cel pracy	Steganografia sieciowa to popularny aktualnie temat prac badawczych. Odpowiada za nadużycie istniejącego kanału komunikacyjnego w taki sposób, aby pośród legalnych danych przesłać dodatkowe, ukryte informacje. Najprostsza klasyfikacja steganografii to kanały pojemnościowe i czasowe. Typowe podejście do eliminacji ukrytych kanałów to detekcja, określenie typu i następnie eliminacja. Celem pracy jest opracowanie i przetestowanie rozwiązania opartego o serwer pośredniczący (proxy) pod względem możliwości eliminacji ukrytych kanałów – pojemnościowych i czasowych. Nowym aspektem pracy będzie zbadanie możliwości eliminacji potencjalnego ukrytego kanału bez uprzedniej detekcji.
Zadania	W ramach pracy przewiduje się realizację następujących zadań: 1. Przegląd i klasyfikacja metod steganografii sieciowej 2. Przegląd rozwiązań serwerów pośredniczących, które mogą zostać wykorzystane do eliminacji kanałów czasowych 3. Projekt i implementacja autorskiego, lub bazującego na istniejącym, rozwiązania serwera proxy 4. Badanie i dokumentacja wyników eliminacji znanych ukrytych kanałów
Literatura	1. Elsadig, M. A., Fadlalla, Y. A.: Survey on covert storage channel in computer network protocols: Detection and mitigation techniques. International Journal of Advances in Computer Networks and Its Security, 6(3), 11-17, 2016 2. Mazurczyk, W., Caviglione, L.: Steganography in modern smartphones and mitigation techniques. IEEE Communications Surveys & Tutorials, 17(1), 2014 3. WENDZEL, S., et al.: Pattern-based survey and categorization of network covert channel techniques. ACM Computing Surveys (CSUR), 2015, 47.3: 50 4. Zander, S., Armitage, G., & Branch, P.: A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials, 9(3), 44-57, 2007

Temat 17	Ocena możliwości wykorzystania detekcji oraz inspekcji ruchu szyfrowanego do zwalczania złośliwego oprogramowania
Temat w języku angielskim	Feasibility study on encrypted traffic inspection and detection to fight malware
Opiekun pracy	dr inż. Tomasz Gierszewski
Konsultant pracy	

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Cel pracy	Inspekcja ruchu szyfrowanego stanowi istotny element zwalczania złośliwego oprogramowania. Pozwala między innymi wychwytywać szereg zagrożeń tzw. drive-by, gdzie malware próbuje ściągnąć kolejny swój element na stację ofiary poprzez szyfrowany tunel. Istniej jednak próby szyfrowania ruchu sieciowego w sposób nieszablonowy, który wprost nie poddaje się inspekcji. Tezą pracy jest możliwość detekcji takiego ruchu, który jest zaszyfrowany, ale wprost nie poddaje się inspekcji. Celem pracy jest implementacja narzędzia PoC, które pozwoli albo wykonać inspekcję ruchowi szyfrowanemu malware, albo zablokuje taką komunikację.
Zadania	W ramach pracy przewiduje się realizację następujących zadań: 1. Przegląd Open Source narzędzi inspekcji ruchu SSL/TLS – w wersjach MitM oraz serwerów pośredniczących (proxy) 2. Analiza sposobów detekcji zaszyfrowanej komunikacji malware ze szczególnym uwzględnieniem technik uczenia maszynowego 3. Projekt i implementacja rozwiązania inspekcji lub blokowania szyfrowanej komunikacji
Literatura	1. Anderson, B., Paul, S., McGrew, D.: Deciphering malware's use of TLS (without decryption). Journal of Computer Virology and Hacking Techniques, 14(3), 195-211, 2018 2. Anderson, B., McGrew, D.: Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1723-1732), 2017 3. Anderson, B., McGrew, D.: Identifying encrypted malware traffic with contextual flow data. In Proceedings of the 2016 ACM workshop on artificial intelligence and security (pp. 35-46), 2016 4. dokumentacja rozwiązania SSLH 5. dokumentacja Open Source rozwiązań pozwalających wykonać inspekcję ruchu szyfrowanego – Squid, SSLSplit, MitmProxy itp.

Temat 18	Ocena możliwości wykorzystanie koncepcji Internetu Rzeczy w systemach obsługi wołań w niebezpieczeństwie
Temat w języku angielskim	Evaluation of the possibility of using the concept of the Internet of Things in the systems of handling cries in danger
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem pracy jest ocena możliwości wykorzystanie koncepcji Internetu Rzeczy w systemach obsługi wołań w niebezpieczeństwie
Zadania	1. Scharakteryzowanie podstawowych cech systemów, które pozwalają na zakwalifikowanie ich do kategorii Internet Rzeczy. 2. Zapoznanie z problemami projektowania i realizacji sieci typu Internet Rzeczy. 3. Zapoznanie się z rozwiazaniami systemów obsługi wołań w niebezpieczeństwie. 4. Ocena roli Internetu Rzeczy (IoT) w monitoringu nadzorowanych obszarów 5. Mozliwosci wykorzystania IoT w przypadku wypadku samochodowego 6. Zaproponowanie scenariuszy działań w sytuacjach krytycznych wykorzytujacych IoT. 7. Implemetacja wybranego scenariusza 8. Porównanie rozwiązań klasycznych z rozwiazaniami wykorzystujacymi koncepcje IoT

Literatura	1. Krawczyk H., Kaczmarek S., Nowicki K.: Aplikacje i usługi a technologie sieciowe, Wydawnictwo Naukowe PWN, Warszawa 2018 2. Nowicki K., Piechowski O.: Poradnik dla początkujących twórców systemów IoT, AEZ 2018 3. Miller M.: Internet rzeczy, WN PWN, 2016 4. Nowicki K., Uhl T.: Internet Rzeczy a internetowy protokół sieciowy IP// Innowacje, pomiary i bezpieczeństwo w elektroenergetyce/ ed. dr hab. inż. Stanisław Czapp Gdańsk: INFOTECH, WEIA PG, WETI PG, ZP Gdynia, SPE, 2017, s.40-44 5. Batalla J.M, Mastorakis G., Mavromoustakis C.X., Pallis E.: Beyond the Internet of Things: Everything Interconnected, Springer, 2017. 6. 14. Perera C., Zaslavsky A., Christen P., Georgakopoulos D.: Context Aware Computing for The Internet of Things: A Survey, IEEE Communnications Surveys & Tutorials, May, 2013. 7. 15. McCann J., Bryson D.: Smart Clothes and Wearable Technology, Woodhead Publishing, 2009. 8. Loreto S., Romano S.P.: Real-Time Communications in the Web: Issues, Achievements, and Ongoing Standardization Efforts, IEEE Internet Computing, Vol. 16, Iss. 5, 2012.

Temat 19	Ocena wpływu parametrów QoE na współczynnik churn
Temat w języku angielskim	Assessment of the influence of QoE parameters on the churn factor
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	mgr inż. Izabela Mazur
Cel pracy	1. Przegląd dotychczasowych badań nad wpływem QoE na churn. 2. Opracowanie metody badań nad wpływem QoE na churn. 3. Przeprowadzenie badania. 4. Analiza uzyskanych rezultatów.
Zadania	1. Przegląd dotychczasowych badań nad wpływem QoE na churn. 2. Opracowanie metody badań nad wpływem QoE na churn. 3. Przeprowadzenie badania. Analiza uzyskanych rezultatów.
Literatura	• Mazur I., Rak J., Nowicki K. (2020) „Minimising the Churn out of the Service by Using a Fairness Mechanism” • Shaikh, J., Fiedler, M., & Collange, D. (2010). “Quality of Experience from user and network perspectives.” annals of telecommunications - annales des télécommunications, 65, 47-57. • ITU-T: Recommendation P.800 – Methods for subjective determination of trans-mission quality, International Telecommunication Union (1996)

Temat 20	Porównanie rozwiązań typu open-source do monitorowania klastra Kubernetes w środowisku produkcyjnym

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Temat w języku angielskim	Comparison of open-source monitoring solutions for Kubernetes cluster in a production environment
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	Kubernetes jest obecnie jednym z najpopularniejszych narzędzi realizujących zadanie orkiestracji kontenerów, powszechnie wykorzystywanym w środowiskach produkcyjnych. Duża funkcjonalność powyższego rozwiązania i w efekcie stale powiększająca się ilość produktów przenoszonych z jego użyciem do środowiska chmurowego czyni potrzebę kompleksowego monitorowania zużycia zasobów szczególnie ważnym aspektem tego rodzaju wdrożeń. Celem pracy jest porównanie istniejących rozwiązań open-source przeznaczonych do monitorowania wykorzystania zasobów w środowisku klastra Kubernetes. Analiza powinna przedstawić wymagania specyficzne dla środowiska produkcyjnego stawiane przed monitoringiem oraz stopień i sposób ich realizacji przez rozwiązania będące przedmiotem badań. Wybrane aspekty funkcjonowania powyższych rozwiązań zostaną przedstawione w postaci demonstratora stworzonego w środowisku laboratoryjnym.
Zadania	• Analiza wymagań dotyczących rozwiązań monitorowania w środowisku produkcyjnym na klastrze Kubernetes. • Przegląd rozwiązań open-source pod kątem zastosowań w środowisku produkcyjnym względem wcześniej określonych wymagań. • Demonstracja kluczowych funkcji i mechanizmów w środowisku laboratoryjnym.
Literatura	• Cloud Native DevOps with Kubernetes. Building, Deploying, and Scaling Modern Applications in the Cloud / John Arundel, Justin Domingus. 2019 • Kubernetes - Dokumentacja, https://kubernetes.io/pl/docs/home/ • Prometheus - Docs, https://prometheus.io/docs/ • Grafana documentation,https://grafana.com/docs/grafana/latest/

Temat 21	Projekt niezawodnego systemu sieciowego odpornego na umyślne działania niszczące
Temat w języku angielskim	Design of a resilient networked system resistant to malicious human activities
Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Cel pracy	Celem pracy jest zaprojektowanie architektury systemu sieciowego (w tym architektury sieci i lokalizacji centrów obliczeniowych/centrów danych) o wysokim stopniu odporności przed atakami
Zadania	• przegląd literatury odnośnie istniejących projektowania sieci i systemów sieciowych o zwiększonej odporności na ataki • projekt rozwiązania własnego • implementacja narzędzia weryfikacji architektury • weryfikacja symulacyjna właściwości rozwiązania własnego w zestawieniu z rozwiązaniem referencyjnym

Literatura	• artykuły z bazy IEEE Xplore • literatura podana przez opiekuna pracy

Temat 22	Przegląd i analiza mechanizmów tworzenia wirtualnych struktur sieciowych w systemie OpenStack
Temat w języku angielskim	Analysis of network virtualization mechanisms of OpenStack system
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	System OpenStack stanowi przykład kompleksowego podejścia do tworzenia, utrzymania i wykorzystania systemów chmurowych – zawiera elementy pozwalające na realizację różnorodnych funkcji, począwszy od automatycznej instalacji i konfiguracji nowych elementów fizycznych, poprzez świadczenie usług IaaS, a kończąc na orkiestracji aplikacji skonteneryzowanych. Jednym z kluczowych elementów koniecznych do realizacji powyższych funkcji jest obsługa wirtualnych struktur sieciowych. Celem pracy jest dokonanie przeglądu funkcjonalności systemu OpenStack w tym zakresie oraz wykorzystywanych w tym celu mechanizmów i wskazanie ich zastosowań w dostarczaniu usług chmurowych. Wybrane funkcje i mechanizmy powinny zostać przetestowane w środowisku laboratoryjnym.
Zadania	• Przegląd i analiza mechanizmów wirtualizacji komunikacji sieciowej w systemie OpenStack. • Porównanie funkcjonalności i efektywności działania wybranych mechanizmów tworzenia wirtualnych struktur sieciowych. • Demonstracja kluczowych funkcji i mechanizmów w środowisku laboratoryjnym.
Literatura	• James Denton, Learning OpenStack Networking - Third Edition, Packt Publishing, 2018 • Kevin Jackson, Cody Bunch, Egle Sigler and James Denton, OpenStack Cloud Computing Cookbook - Fourth Edition, Packt Publishing, 2018

Temat 23	Przegląd i analiza popularnych środowisk orkiestracji aplikacji skonteneryzowanych
Temat w języku angielskim	Comparison and analysis of popular orchestration systems for containerized applications
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	Wdrażanie aplikacji w postaci skonteneryzowanej jest dziś bardzo popularnym rozwiązaniem w systemach chmurowych. Wiąże się z tym dostępność wielu rozwiązań wspomagających ten proces i oferujących mechanizmy wspomagające obsługę kompletnego cyklu życia aplikacji w interesującym nas środowisku. Celem pracy jest dokonanie przeglądu oraz porównania wybranych produktów tego rodzaju.

	Analiza powyższa powinna umożliwiać określenie oczekiwanej od tego rodzaju produktów funkcjonalności, wskazanie ich zalet i wad ora zalecanych scenariuszy ich wykorzystania.
Zadania	• Przegląd i analiza popularnych rozwiązań orkiestracji aplikacji skonteneryzowanych. • Porównanie funkcjonalności oferowanych przez powyższe rozwiązania oraz zalecanych scenariuszy i sposobów ich wykorzystania. • Badania wybranych produktów i scenariuszy w środowisku laboratoryjnym.
Literatura	• Randall Smith, Docker Orchestration, Packt Publishing, 2017 • Hideto Saito, Hui-Chuan Chloe Lee and Cheng-Yang Wu, DevOps with Kubernetes - Second Edition, Packt Publishing 2019

Temat 24	Przegląd narzędzi do zarządzania konfiguracją i realizacji usług Infrastructure as a Code w środowisku chmur obliczeniowych
Temat w języku angielskim	Comparison of configuration management and Infrastructure as Code tools in cloud infrastructure
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Cel pracy	Automatyzacja konfiguracji infrastruktury chmurowej jest obecnie wyzwaniem, z którym musi zmierzyć się wiele firm informatycznych. Jego realizacja wymaga najczęściej zastosowania wielu różnych narzędzi, z pośród których narzędzia związane z tworzeniem konfiguracji oraz zarządzaniem konfiguracją pełnią kluczową rolę, a odpowiedni ich wybór ma zasadnicze znaczenie. Celem pracy jest porównanie istniejących rozwiązań typu open-source oraz specyficznych dla dostawców chmurowych, przeznaczonych do zarządzania konfiguracją oraz realizacji rozwiązań typu Infrastracture as a Code. Analiza powinna obejmować funkcjonalność narzędzi pod kątem możliwości tworzenia oraz konfiguracji infrastruktury IT w środowiskach chmurowych.
Zadania	• Przegląd wybranych narzędzi do zarządzania konfiguracją oraz realizacji usługi Infrastructure as a Code • Przygotowanie przykładowych konfiguracji testowych i weryfikacja działania narzędzi w środowisku laboratoryjnym • Określenie zalecanych scenariuszy użycia rozważanych narzędzi w zależności od rodzaju tworzonych środowisk oraz dostawcy chmurowego
Literatura	• Infrastructure as Code: Managing Servers in the Cloud / Kief Morris 2016 • Ansible w Praktyce: Automatyzacja konfiguracji i proste instalowanie systemów. Wydanie II. / Lorin Hochstein, Rene Moser 2018 • Terraform: Up & Running. Writing Infrastructure as Code . 2nd Edition. / Yevgeniy Brikman 2019 • Materiały udostępniane przez operatorów systemów chmurowych, np.: Amazon Web Services, Google Cloud Platform, Microsoft Azure

Temat 25	Realizacja metody niezawodnej transmisji informacji w sieci FSO (Free Space Optical) odpornej na zakłócenia spowodowane czynnikam pogodowymi
Temat w języku angielskim	A routing scheme for FSO (Free Space Optical) networks resilient to weather-induced disruptions

Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Cel pracy	Celem pracy jest opracowanie metody niezawodnej transmisji informacji dla architektury Free Space Optical (sieci bezprzewodowej z węzłami stacjonarnymi i transmisją bezprzewodową optyczną) odpornej na zakłócenia spowodowane czynnikami pogodowymi (takimi jak opady deszczu)
Zadania	• przegląd literatury odnośnie istniejących metod niezawodnej transmisji w sieciach FSO dla scenariuszy zakłóceń spowodowanych czynnikami pogodowymi • projekt rozwiązania własnego • implementacja symulatora • weryfikacja symulacyjna właściwości rozwiązania własnego w zestawieniu z rozwiązaniem referencyjnym
Literatura	• artykuły z bazy IEEE Xplore • literatura podana przez opiekuna pracy

Temat 26	Realizacja metody niezawodnej transmisji informacji w zastosowaniach sieci z transmisją odporną na opóźnienia
Temat w języku angielskim	A scheme of a resilient routing for Delay-tolerant Networks
Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Cel pracy	Celem pracy jest opracowanie metody niezawodnej transmisji informacji w sieci z transmisją odporną na opóźnienia (DTN) sieci z transmisją odporną na opóźnienia (DTN)
Zadania	• przegląd literatury odnośnie istniejących metod transmisji w sieciach DTN • projekt rozwiązania własnego • implementacja symulatora • weryfikacja symulacyjna właściwości rozwiązania własnego w zestawieniu z rozwiązaniem referencyjnym
Literatura	• artykuły z bazy IEEE Xplore • literatura podana przez opiekuna pracy

Temat 27	Realizacja metody szybkiego odtworzenia transmisji po awarii w sieciach IP
Temat w języku angielskim	Design and implementation of a fast rerouting scheme for IP networks
Opiekun pracy	dr hab. inż. Jacek Rak

Konsultant pracy	
Cel pracy	Celem pracy jest opracowanie metody niezawodnej transmisji informacji w sieciach IP umożliwiającej szybkie wznowienie transmisji po awarii elementu sieci
Zadania	• przegląd literatury odnośnie istniejących metod szybkiego przekierowania transmisji w sieciach IP • projekt rozwiązania własnego • implementacja symulatora • weryfikacja symulacyjna właściwości rozwiązania własnego w zestawieniu z rozwiązaniem referencyjnym
Literatura	• artykuły z bazy IEEE Xplore • literatura podana przez opiekuna pracy

Temat 28	Realizacja metody ochrony transmisji w sieci teleinformatycznej przed awarią masową uwarunkowaną umyślnym działaniem niszczącym
Temat w języku angielskim	Design and implementation of a method of resilient routing for the scenario of massive failures following from a malicious human activity
Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Cel pracy	Celem pracy jest opracowanie metody doboru tras (routingu), która zapewniałaby ciągłość transmisji po awarii masowej będącej następstwem umyślnego działania niszczącego
Zadania	• przegląd literatury odnośnie istniejących koncepcji ochrony transmisji informacji dla scenariusza awarii masowej w wyniku umyślnego działania niszczącego • projekt i weryfikacja właściwości rozwiązania własnego w zestawieniu z rozwiązaniem referencyjnym
Literatura	• artykuły z bazy IEEE Xplore • literatura podana przez opiekuna pracy

Temat 29	Strategie obrony sieci bezprzewodowych o topologii wieloskokowej przed inteligentnymi atakami metodą podmiany klasy ruchu
Temat w języku angielskim	Defense strategies against intelligent traffic class remapping attacks in multi-hop wireless networks
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	

POLITECHNIKA GDAŃSKA

3 czerwca 2020

Cel pracy	Celem pracy jest zbadanie, czy ataki na poziomie podwarstwy MAC mogą mieć zasięg większy niż najbliższe sąsiedztwo węzła atakującego oraz ocena efektów takich ataków i skuteczności mechanizmów obronnych.
Zadania	1. Zapoznanie się z metodami wsparcia QoS w sieciach bezprzewodowych o topologii wieloskokowej oraz sposobami ich wykorzystanie przez węzły atakujące 2. Opracowanie symulacyjnego modelu ataku wykorzystującego mechanizm EDCA 3. Opracowanie symulacyjnego modelu sieci z atakami na wiele przepływów pakietowych 4. Symulacja wybranych strategii ataków i ocena skuteczności obronnej mechanizmów sterowania ruchem
Literatura	1. J. Konorski, S. Szott, Discouraging traffic remapping attacks in local ad hoc networks, IEEE Trans Wireless Communications, 2014, 3752-3767. 2. R. Haywood, S. Mukherjee, X.-H. Peng, Investigation of H.264 Video Streaming over an IEEE 802.11e EDCA Wireless Testbed, IEEE International Conf. on Communications, 2009. 3. S. Szott, M. Natkaniec, A. R. Pach, Improving QoS and security in wireless ad hoc networks by mitigating the impact of selfish behaviors: a game-theoretic approach, Security and Communication Networks 6 (2013) 509-522. 4. Inne materiały źródłowe dostępne u opiekuna

Temat 30	Zastosowanie uczenia maszynowego do projektowania strategii ataku metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług
Temat w języku angielskim	**Application of machine learning for the design of Fake VIP attack strategies in computer communication systems supporting QoS differentiation**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Cel pracy	W systemach teleinformatycznych wspierających różnicowanie jakości usług (QoS) atak metodą fałszywego VIPa jest odmianą niewykrywalnej uzurpacji uprawnień. W obliczu żądania usług agent IDS może zrezygnować z kosztownej procedury weryfikacji sygnatury żądania i okazać mu zaufanie, przydzielając żądany poziom QoS. Celem pracy jest odpowiedź na pytanie, czy zastosowanie sztucznej inteligencji z ograniczoną informacją zwrotną od agenta IDS pomoże w opracowaniu lepszych strategii ataku niż oczywiste strategie probabilistyczne.
Zadania	1. Opracowanie formalizmu ataku metodą fałszywego VIPa w różnych środowiskach systemów informatycznych 2. Analiza dostępnej informacji zwrotnej od agenta IDS 3. Pozyskanie zbiorów danych wejściowych do eksperymentów 4. Analiza możliwości wykorzystania znanych algorytmów AI, w tym głębokiego uczenia.

Literatura	1. Y. L. Sun, Y. Liu, *Security of online reputation systems: The evolution of attacks and defenses*, IEEE Signal Proc. Mag., vol. 29, 201 2. Po-Ching Lin et al., *Using String Matching for Deep Packet Inspection*, Computer, vol. 41, 2008 3. Patcha, Jung-Min Park, *A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks*, Int. J. of Network Security vol. 2, 2006. 4. T. Grandison and M. Sloman, *A survey of trust in internet applications*, IEEE Comm. Surveys & Tutorials, vol. 3, 2000. 5. I. Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press 2016 6. inne materiały źródłowe dostępne u opiekuna

Temat 31	Analiza mechanizmów zapewniania skalowalności sieci Ethetnet
Temat w języku angielskim	Analysis of mechanisms to ensure the scalability of the Ethernet network
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Cel pracy	Celem pracy jest analiza mechanizmów zapewniania skalowalności sieci Ethernet
Zadania	1. Przegląd mechanizmów zapewniania skalowalności sieci Ethernet, w szczególności – szczegółowy opis autonegocjacji, QinQ, MACinMAC, usług MEF 2. Zaproponowanie modyfikacji wybranego mechanizmu zapewniania skalowalności sieci Ethernet 3. Implementacja zaproponowanej modyfikacji (albo w systemie rzeczywistym alblbo w systemie zwirtualizowanym albo w symulatorze) 4. Porównanie klasycznych i zmodyfikowanych rozwiązań
Literatura	1. Nowicki K., Uhl T.: Monitorowanie i bezpieczeństwo sieci komputerowych. Szczecin: Wydawnictwo Naukowe Akademii Morskiej w Szczecinie, 2016.148 s. ISBN 970−83−64434−08−2 2. Nowicki K., Uhl T.: Ethernet end-to-end. Eine universelle Netzwerktechnologie. Aachen: Shaker Verlag, 2008. 225 s. ISBN 978-3-8322-7140-4 3. Nowicki K.: Ethernet - sieci, mechanizmy. Gdańsk: INFOTECH, 2006.152 s. ISBN 83-921711-2-8 4. Nowicki K., Malinowski A..: Topology Discovery of Hierarchical Ethernet LANs without SNMP support, W: The 41st Annual Conference of the IEEE Industrial Electronics Society, 2015, IEEE Industrial Electronics Society 5. Nowicki K., Ostrowski A., Poźniak A., Wrzesiński Ł.: Wykorzystanie sprzętu komputerowego klasy SOHO do modelowania złożonych rozwiązań sieciowych// STUDIA INFORMATICA. SYSTEMS AND INFORMATION TECHNOLOGY. SYSTEMY I TECHNOLOGIE INFORMACYJNE. -Vol. 32., nr. Nr 3A (98) (2011), s.55-66

6. Allan D., Bragg N.: 802.1aq Shortest Path bridging. Design and Evolution, Willey, IEEE, 2012
7. http://standards.ieee.org/findstds/index.html