KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo sieci definiowanych programowo

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	15	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Mariusz Żal

mariusz.zal@put.poznan.pl

tel: 61 665 39 26

Wydział Informatyki i Telekomunikacji

Instytut Sieci Teleinformatycznych

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć podstawową wiedzę z zakresu sieci komputerowych, protokołów routingu, bezpieczeństwa teleinformatycznego oraz podstaw programowania w językach Java i C/C++. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom wiedzy z zakresu szeroko rozumianych sieci definiowanych przez oprogramowanie SDN (Software Define Network), wirtualizacji funkcji sieciowych (NFV) oraz wyzwań w zakresie bezpieczeństwa jakie stawione są twórcom i administratorom tych sieci. Przedstawione zostaną sposoby analizy zdarzeń zachodzących w SDN oraz NFV w celu detekcji zagrożeń i ataków. Omawiane

zagadnienia będą uzupełnieniem wiedzy w zakresie bezpieczeństwa w sieciach komputerowych a nie ich powtórzeniem. Zapoznanie z wyzwaniami, jakie stawiane są płaszczyzną aplikacji, sterowania i danych. Przedstawienie języka P4 wraz z wykorzystywanymi modelami przełączników i kart sieciowy w zakresie tworzenia bezpiecznych rozwiązań sieciowych.

W ramach realizacji przedmiotu przedstawione zostaną rozwiązania poprawiające bezpieczeństwo sieci definiowanych programowo oraz wirtualizacji funkcji sieciowych oraz zaawansowane strategie takie, jak mikrosegmentacja, MTD oraz ochrona inteligentnych sieci SDN. Omówione zostaną standardy ITU-T, ETSI oraz IETF w zakresie bezpieczeństwa sieci oraz kierunki rozwoju.

Przedmiotowe efekty uczenia się

Wiedza

Ma zaawansowaną i pogłębioną wiedzę z zakresu bezpieczeństwa sieci definiowanych programowo oraz wirtualizacji funkcji sieciowych oraz metod, narzędzi i środowisk programistycznych wykorzystywanych do zbierania danych, analizy oraz detekcji zagrożeń i ataków w tych sieciach.

Ma zaawansowaną wiedzę szczegółową dotyczącą rozwiązań i strategii bezpieczeństwa w sieciach definiowanych programowo.

Ma wiedzę o kierunkach rozwoju rozwiązań i strategii bezpieczeństwa w sieciach definiowanych programowo i najistotniejszych zaleceniach dotyczących szeroko rozumianego bezpieczeństwa sieci SDN.

Ma zaawansowaną i szczegółową wiedzę o procesach zachodzących w cyklu życia mechanizmów bezpieczeństwa NFV.

Umiejętności

Potrafi pozyskiwać informacje z literatury oraz zaleceń (w języku polskim i angielskim) na temat bezpieczeństwa sieci SDN oraz NFV, integrować je, dokonywać ich interpretacji i krytycznej oceny.

Potrafi wykorzystać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych w obszarze bezpieczeństwa sieci SDN i NFV.

Potrafi — przy formułowaniu i rozwiązywaniu zadań inżynierskich — integrować wiedzę z różnych obszarów informatyki, w tym programowania oraz zasad działania sieci komputerowych w celu budowy bezpiecznych sieci definiowanych programowo oraz implementacji wirtualnych funkcji sieciowych, które są odporne na różne formy ataków.

Potrafi ocenić przydatność i możliwość wykorzystania nowych rozwiązań sprzętowych i programowych służących do rozwiązywania zadań inżynierskich, polegających na projektowaniu i implementacji bezpiecznych sieci definiowanych programowo oraz implementacji wirtualnych funkcji sieciowych.

Potrafi porozumiewać się w języku polskim i angielskim przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach, także z wykorzystaniem narzędzi informatycznych

Potrafi współdziałać w zespole odpowiedzialnym za zapewnienie bezpieczeństwa systemom teleinformatycznym.

Potrafi określić kierunki dalszego uczenia się w celu sprostania wyzwaniom stawianym osobom odpowiedzialnym za bezpieczeństwo systemów teleinformatycznych.

Kompetencje społeczne

Rozumie, że w zakresie bezpieczeństwa sieci SDN i NFV wiedza i umiejętności bardzo szybko stają się przestarzałe.

Rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu bezpieczeństwa sieci SDN i NFV w rozwiązywaniu problemów badawczych i praktycznych.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta w ramach wykładu weryfikowana jest przez egzamin w formie pisemnej lub ustnej. W formie pisemnej studenci muszą udzielić odpowiedzi na 7 - 10 pytań (testowych i otwartych) różnie punktowanych. Są trzy lub cztery grupy punktowe. Natomiast w przypadku egzaminu ustnego student losuje po jednym pytaniu z każdej grupy punktowej. W formie ustnej, do każdego wylosowanego pytania, student może otrzymać dodatkowe pytanie (związane z wylosowanym pytaniem). Ocena pytania (obejmuje odpowiedź zarówno na pytanie wylosowane jak i pytanie dodatkowe) obejmuje zakres odpowiedzi oraz głębię zrozumienia zagadnienia. Do każdego egzaminu przygotowywanych jest 50 - 60 pytań. Warunkiem pozytywnego zaliczenia egzaminu otrzymanie minimum 50% punktów możliwych do zdobycia.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco. Na każdych zajęciach laboratoryjnych oceniana jest poprawność wykonania ćwiczeń w skali od 0 do 10 punktów.Warunkiem pozytywnego zaliczenia ćwiczeń laboratoryjnych jest otrzymanie minimum 50% punktów możliwych do zdobycia.

liczba punktów	ocena
<=50 %	2,0
51% - 60%	3,0
61% - 70%	3,5
71% - 80%	4,0
81% - 90%	4,5
91% - 100%	5,0

Treści programowe

Tematyka wykładów:

- Sieci definiowane przez oprogramowanie - wprowadzenie, definicje, architektury.
- Przegląd rozwiązań i implementacji sieci SDN
- Analiza bezpieczeństwa oraz wykrywanie ataków w SDN:
  - Warstwa aplikacji,

- Płaszczyzna sterowania,
- Płaszczyzna danych.

• Wektory zagrożeń w sieciach SDN
• Systemy głęboko programowalne– bezpieczeństwo w języku P4
• Wirtualizacji funkcji sieciowych NFV – struktura, implementacje
• Wyzwania w zakresie bezpieczeństwa stawiane NFV: klasyfikacja zabezpieczeń, cykl życia zabezpieczeń
• Bezpieczeństwo SDN i NFV w zastosowaniach przemysłowych - przegląd standardów oraz zaleceń
• Przegląd rozwiązań dla typowych zagrożeń w sieciach SDH:
- Nieaytoryzowany dostęp,
- Złośliwe aplikacje,
- DoS
- Błędna konfiguracja
- Zabezpieczenia w SDN na poziomie systemu
• Zaawansowane rozwiązania dla bezpieczeństwa sieci SDN:
- Mikrosegmentacja
- Ruchoma obrona celu
- Reprezentacja ataku
- Łańcuchy funkcji usługowych
- AI w bezpieczeństwie SDN
•Sieci definiowane bezpieczeństwem - przyszłe kierunki rozwoju

Tematyka laboratoriów:
Zgodna z treściami wykładów

Metody dydaktyczne

Wykład informacyjny: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach, z wykorzystaniem fizycznych urządzeń sieciowych oraz środowisk wirtualnych.

Literatura

Podstawowa

1. Khondoker, Rahamatullah (Ed.): SDN and NFV Security - Security Analysis of Software-Defined Networking and Network Function Virtualization; Springer International Publishing 2018.

2. Guy Pyjolle: Software Networks: Virtualization, SDN, 5G and Security, John Wiley & Sons, 2015

Uzupełniająca

1.Shao Ying Zhu, Sandra Scott-Hayward, Ludovic Jacquin, Richard Hill: Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications. Computer Communications and Networks, Springer 2017.

2. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody: Software-Defined Networking and Security - From Theory to Practice, CRC Press, 2021

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	75	3,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu)[1]	45	1,5

[1] niepotrzebne skreślić lub dopisać inne czynności