KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Algorytmy uwierzytelniania i autoryzacji w systemach bezprzewodowych [S1MiKC1E>AUiAwSB]

Przedmiot

Kierunek studiów
Mikroelektronika i komunikacja cyfrowa/ Microelectronics and Digital Communication

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
15

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
15

Liczba punktów ECTS

2,00

Koordynatorzy

dr hab. inż. Piotr Remlein
piotr.remlein@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynając ten kurs powinien posiadać podstawową wiedzę z zakresu systemów telekomunikcyjnych. Ponadto powinien posiadać podstawową wiedzę o sieciach teleinformatycznych, podstawowe umiejętności konfiguracji urządzeń sieciowych oraz rozumieć proces komunikacji pomiędzy urządzeniami sieciowymi. Student powinien posiadać podstawowe umiejętności programowania a także pozyskiwania informacji ze wskazanych źródeł.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z podstawowymi metodami uwierzytelniania i autoryzacji użytkowników, urządzeń oraz systemów w różnych środowiskach technologicznych. Przedmiot obejmuje zarówno teoretyczne aspekty bepieczeństwa, uwierzytelniania, jak i praktyczne zastosowania w kontekście współczesnych zagrożeń bezpieczeństwa w różnych systemach teleinformatycznych w tym sieciach komórkowych i innych systemach bezprzewodowych.

Przedmiotowe efekty uczenia się

Wiedza:

Zna podstawowe pojęcia i definicje z zakresu uwierzytelniania i autoryacji. Rozumie różnicę między identyfikacją, uwierzytelnianiem a autoryzacją. Potrafi wyjaśnić rolę uwierzytelniania w systemach bezpieczeństwa.
Zna różne metody uwierzytelniania. Potrafi scharakteryzować metody statyczne, biometryczne, oparte na tokenach oraz wieloskładnikowe. Rozumie mechanizmy uwierzytelniania oparte na protokołach, np. OAuth, Kerberos, SAML, 802.1X.
Zna zagrożenia związane z systemami uwierzytelniania. Rozumie ataki, takie jak np.: brute force, phishing czy credential stuffing, oraz zna sposoby przeciwdziałania im. Zna znaczenie ochrony danych uwierzytelniających poprzez szyfrowanie i inne środki zabezpieczające.
Zna zastosowania systemów uwierzytelniania w różnych systemach i środowiskach. Rozumie specyfikę uwierzytelniania w systemach przewodowych i bezprzewodowych, aplikacjach mobilnych, chmurze sieciach sensorowych, IoT.

Umiejętności:
Student potrafi dobrać odpowiednie metody uwierzytelniania do konkretnego zastosowania. Analizuje wymagania bezpieczeństwa i środowisko aplikacji w celu zaprojektowania właściwego systemu uwierzytelniania. Umie zaprojektować i skonfigurować systemy wykorzystujęce metody wierzytelnia. Umie rozwiązać praktyczne problemy związane z uwierzytelnianiem. Potrafi przeprowadzić symulację ataków na systemy uwierzytelniające i ocenić ich odporność. Umie przygotować raport oceniający efektywność zastosowanych mechanizmów uwierzytelninia i zarządzania kluczami.

Kompetencje społeczne:
Rozumie odpowiedzialność za projektowanie bezpiecznych systemów uwierzytelniania. Uznaje znaczenie ochrony danych osobowych i poufności informacji w kontekście uwierzytelniania. Podejmuje decyzje uwzględniające bezpieczeństwo użytkowników końcowych. Potrafi pracować w zespole projektowym. Potrafi efektywnie komunikować wyniki analiz oraz propozycje ulepszeń w zakresie uwierzytelniania. Dąży do ciągłego poszerzania wiedzy z zakresu bezpieczeństwa systemów informatycznych: Śledzi aktualne zagrożenia i nowe metody uwierzytelniania w dynamicznie zmieniającym się środowisku technologicznym.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na podstawie zaliczenia przeprowadzonego w postaci pisemnej lub ustnej, lub też w postaci testu. Próg zaliczeniowy wynosi 51% punktów. Zaliczenie projektu odbywa się także na podstawie zdobycia co najmniej 50% możliwych do uzyskania punktów. Skala ocen: <50% - 2,0 (ndst); 50% do 59% - 3,0 (dst); 60% do 69% - 3,5 (dst+) ; 70% do 79% - 4,0 (db); 80% do 89% - 4,5 (db+); 90% do 100% - 5,0 (bdb).

Treści programowe

Przedmiot obejmuje zagadnienia związane z identyfikacją, uwierzytelnieniem i autoryzacją użytkowników, autoryzacją dostępu oraz ochroną danych w systemach informatycznych i sieciach przewodowych i bezprzewodowych. Omawiane są różne metody uwierzytelniania, w tym wykorzystanie haseł, tokenów, biometrii oraz mechanizmów wieloskładnikowych (MFA). W ramach przedmiotu omawiane są również kluczowe protokoły, takie jak 802.1X, Kerberos, OAuth 2.0 czy OpenID Connect, oraz ich zastosowanie w zapewnianiu bezpieczeństwa.
W zakresie zarządzania kluczami studenci poznają procesy generowania, przechowywania, dystrybucji i rotacji kluczy kryptograficznych, ze szczególnym uwzględnieniem infrastruktury klucza publicznego (PKI). Istotną część kursu stanowi analiza zabezpieczeń komunikacji w tym metod uwierzytelnienia stosowanych w praktycznych systemacj np. telefoni komórkowej GSM, UMT, LTE, 5G, sieciach sensorowych czy IoT. Uwierzytelnienie w systemie TETRA.
Dodatkowo omawiane są zagrożenia, takie jak ataki brute force, man-in-the-middle czy phishing, oraz sposoby ich wykrywania i zapobiegania. Przedmiot porusza także zastosowanie systemów uwierzytelniania w środowiskach IoT, sieciach bezprzewodowych (WPA2, WPA3) oraz chmurze, i rozwiązaniach webowych uwzględniając najnowsze trendy, takie jak passwordless authentication czy kryptografia kwantowa.
W ramach projektu studenci realizują zadania w oparciu o wybrane oprogramowanie realizując określone algorytmy uwierzytelnienia. Dokonują ich oceny i analizy, Mogą wykorzystywać wybrane programy symulacyjne, np. Tamari lub Scyther.

Tematyka zajęć

Wykład:
1. (1h) Wprowadzenie do bepieczeństwa w systemaach bezprzewodowych. (1h)
2. (2h) Wprowadzenie do uwierzytelniania i zarządzania kluczami w sieciach
Podstawowe pojęcia: identyfikacja, uwierzytelnianie, autoryzacja.
Rola zarządzania kluczami w ochronie danych przesyłanych w sieciach.
Rola centralizacji uwierzytelniania w dużych systemach IT.
Powiązanie procesów uwierzytelniania z systemami zarządzania kluczami (KMS - Key Management System).
3. (2h) Metody uwierzytelniania w sieciach przewodowych i aplikacjach webowych
Uwierzytelnianie kontekstowe i bezhasłowe jako przykłady nowych rozwiązań.
Mechanizmy 802.1X i EAP (Extensible Authentication Protocol).
Rola serwera RADIUS w uwierzytelnianiu użytkowników. Wykorzystanie
4. (2h) Uwierzytelnianie w sieciach bezprzewodowych
Mechanizmy uwierzytelniania w standardach WLAN (WPA2, WPA3).
Uwierzytelnianie na poziomie sieci komórkowych (GSM, UMTS, LTE, 5G).
Uwierzytelnienie w systemie TETRA.
Lekkie algorytmy uwierzytelnianie dla sieci sensorowych i IoT
5. (2h) Protokoły uwierzytelniania w sieciach korporacyjnych i publicznych
Kerberos: zasady działania i zastosowanie. Uwierzytelnianie biometryczne.
Zarządzanie kluczami w sieciach przewodowych, bezprzewodowych, w środowiskach chmurowych i IoT: Przykłady rozwiązań (np. AWS KMS, Google Cloud KMS). Zastosowanie nowoczesnych metod uwierzytelnienia.
Wyjątkowe wyzwania związane z zarządzaniem kluczami w środowiskach zdecentralizowanych.
Sposoby generowania, dystrybucji i przechowywania kluczy. Rotacja kluczy i ochrona przed wyciekiem danych.
6. (2h) Infrastruktura Klucza Publicznego (PKI)
Certyfikaty cyfrowe i hierarchia zaufania.
Procesy związane z PKI: rejestracja, unieważnianie i odnawianie certyfikatów.
Składniki PKI: certyfikaty cyfrowe, hierarchia zaufania, urzędy certyfikacji (CA).
Procesy w PKI: wydawanie, odnawianie i unieważnianie certyfikatów.
Rola PKI w systemach uwierzytelniania, np. TLS/SSL, zasady działania tych protokołów.
7. (2h) Ataki na systemy uwierzytelniania i ich przeciwdziałanie. Ochrona przed atakami, np. takimi jak jamming, przechwytywanie transmisji czy spoofing.
Typowe zagrożenia: brute force, man-in-the-middle, replay attack.
Mechanizmy obrony, np. czasowe blokady konta, analizy behawioralne.
8. (2h) Nowoczesne podejścia do uwierzytelniania i zarządzania kluczami
Rozwój systemów bezhasłowych (passwordless authentication).
Potencjalne zastosowanie kryptografii kwantowej w zarządzaniu kluczami.
Projekt:
W ramach projektu należy zaprojektować, zaimplementować wybrane przykładowe algorytmy uwierzytelniania użytkowników, które wykorzystują mechanizmy zarządzania kluczami. Należy dokonać analizy ich działania i złożoności. Dokonać oceny odporności systemu na ataki poprzez symulację w wybranym środowisku testowym, np. Scyther. Oczekiwane rezultaty projektu: dokumentacja zawierająca: opis założeń projektowych i przyjętych rozwiązań technicznych, diagramy architektury systemu, analizę ryzyka i propozycje zabezpieczeń, opis implementacji, testy, przeprowadzone scenariusze testowe uwierzytelniania, raport z analizy skuteczności systemu w kontekście bezpieczeństwa.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna ilustrowana przykładami.
2. Projekt: wykonywanie zadań zleconych przez prowadzącego - ćwiczenia praktyczne, praca zespołowa,korzystanie z oprogramowania i środowisk symulacyjnych

Literatura

Podstawowa:
1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2020.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security Essentials: Applications and

Standards, Pearson, 2020.
3. RFC 5246 - The Transport Layer Security (TLS) Protocol.
4. Literatura z uznanych czasopism naukowych, dokumenty normalizacyjne, strony internetowe producentów urządzeń umieszczane przez prowadzącego na platformie ekursy.

Uzupełniająca:
1. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, CRC Press, 2020.
2. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Cengage Learning, 2021.
3. RFC 4120 - The Kerberos Network Authentication Service (V5), 2005.
4. Roger Grimes, Hacking Multifactor Authentication, Wiley, 2020.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	57	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	25	1,00