Autor: *dr inż. Tomasz Czarnecki, mgr inż. Marcin Golański, dr hab. inż. Mariusz Rawski*

Bezpieczeństwo Systemów i Oprogramowania (BSO)
Software and System Security

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 4
Minimalny numer semestru: 4
Wymagania wstępne, zalecane przedmioty poprzedzające: –
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Celem przedmiotu jest zaznajomienie studentów z podstawami bezpieczeństwa systemów i oprogramowania. Przedstawiona zostanie problematyka bezpieczeństwa sprzętowego i programowego, lokalne i sieciowe systemy wykrywania ataków, ochrona przed nimi, narzędzia analizy zabezpieczeń i monitoringu.

Istotnym elementem przedmiotu jest projekt, w ramach którego zespoły projektowe będą miały za zadanie przeanalizować wybrane zagadnienia związane z bezpieczeństwem systemów i oprogramowania, zaproponować rozwiązania i zweryfikować je w postaci praktycznej realizacji sprzętowej lub programowej.
Projekt realizowany będzie etapowo, każdy etap zaliczany będzie na podstawie raportu.

Treść kształcenia:

WYKŁADY:

1. **Niskopoziomowe techniki przejmowania kontroli nad wykonaniem programu (2 godz.).**
   Ataki wykorzystujące przepełnienie bufora (buffer overflow) i metody obrony przed nimi. Wsparcie sprzętowo–programowe na poziomie kompilatora i systemu operacyjnego.

2. **Techniki zabezpieczania kodu (2 godz.).**

Zaciemnianie kodu programu (obfuscation), ochrona przed debugowaniem, wirtualizacja kodu, Backdoory, Kleptografia, Sandboxing. Ogólny zarys metod łamania.

3. **Technologie obiektowe i komponentowe tworzenia oprogramowania (2 godz.).**
   Narzędzia programistyczne, współczesne środowiska programistyczne.

4. **Strategie rozwoju oprogramowania (2 godz.).**
   Modele cyklu życia, niezawodność oprogramowania, projektowanie oprogramowania godnego zaufania, miary jakości oprogramowania, narzędzia zarządzania jakości.

5. **Inteligentne zarządzania rozwojem oprogramowania (2 godz.)**
   Złożoność, błędy i poka–yoke w procesach rozwoju oprogramowania, Pomyłki jako przyczyny defektów oprogramowania, ocena ryzyka, analiza przyczyn i skutków błędów w dziedzinie oprogramowania.

6. **Bezpieczeństwo systemów telekomunikacyjnych - wprowadzenie do podstawowych pojęć i zagadnień (2 godz.).**
   Model komunikacji w ujęciu podstawowych mechanizmów podnoszących poziom zabezpieczeń. Pojęcia związane z bezpieczeństwem w telekomunikacji. Jak operatorzy dbają o zabezpieczenia transmisji – czy w ogóle o to dbają? Przykłady wykorzystania sprzętowych rozwiązań.

7. **Mechanizmy i protokoły bezpieczeństwa (4 godz.).**
   Omówienie aktualnych mechanizmów oraz protokołów. Architektura stosowanych rozwiązań. Wpływ zagrożeń na polityki bezpieczeństwa w sieciach intra i internet. Rozsądny balans zabezpieczeń. Kierunki rozwoju standaryzacji po uwzględnieniu doświadczeń użytkowników końcowych.

8. **Bezpieczeństwo w mediach bezprzewodowych (2 godz.).**
   Ataki na bezprzewodowe sieci publiczne oraz sieci prywatne. Podstawowe zagrożenia w ujęciu użytkownika końcowego. Rodzaje dostępnych mechanizmów sprzętowych. Podstawowe błędy konfiguracji węzłów bezprzewodowych.

9. **Bezpieczeństwo w relacji do modelu ISO/OSI (2 godz.).**
   (a) Bezpieczeństwo warstwy fizycznej: tendencje i nowe metody zabezpieczeń - zastosowanie zwielokrotnienia MIMO, wykorzystanie inteligentnych anten, wykorzystanie pseudolosowości w przetwarzaniu sygnałów i zarządzaniu kanałami komunikacyjnymi.
   (b) Techniki szerokopasmowe: modulacje cyfrowe, układy nadajników (modulatorów) i odbiorników (demodulatorów), funkcja autokorelacji oraz widmowa gęstość mocy dla sygnałów pseudolosowych PN; systemy szerokopasmowe typu BPSK; systemy szerokopasmowe FH.
   (c) Wielodostęp kodowy typu CDMA: model systemu komunikacyjnego, interferencje i zakłócenia sąsiedniokanałowe własne oraz celowe, kryteria wyboru sekwencji pseudolosowych PN.

10. **Mechanizmy zapobiegania podrabianiu modułów sprzętowych i zabezpieczanie rdzeni IP (2 godz.)**
    Zagrożeń związanych z podrabiania modułów sprzętowych. Rodzaje podrabiania modułów sprzętowych (remarked, overproduced, clonned, tempered, itp.). Metody wykrywania. Techniki zapobiegania.

11. **Funkcje fizycznie nieklonowalne PUF i generatory losowe TRNG (2 godz.)**
    Koncepcja funkcji fizycznie nieklonowalnych (Physically Unclonable Function). Zasady działania i wykorzystywane mechanizmy. Zastosowania. Generatory TRNG (True Random Number Generator). Zasady działania i wykorzystywane mechanizmy. Zastosowania

12. **Ataki na moduły sprzętowe i zapobiegnie im (2 godz.)**
    Rodzaje ataków (inwazyjne, nieinwazyjne, półinwazyjne). Reverse Engineering. Ataki typu side-channel. Typy emisji side-channel. Sposoby wykorzystania informacji side-channel. Sposoby zabezpieczania przed atakami side-channel

13. **Trojany sprzętowe (2 godz.)**
    Czym są sprzętowe trojany. Klasyfikacja sprzętowych trojanów i zagrożenia z nimi związane. Problem zaufania w procesie wytwarzania sprzętu (IC/IP Trust Problem). Sposoby detekcji i izolacji sprzętowych trojanów. Zapobieganie wprowadzeniu sprzętowych trojanów do układu.

ĆWICZENIA:
–
LABORATORIA:
–
PROJEKT:

W ramach projektu zespół 2-3 osobowy będzie miał za zadanie przeanalizować wybrane zagadnienie związane z bezpieczeństwem systemu lub oprogramowania, podać konkretne rozwiązanie w postaci procedur, oprogramowania lub zaleceń. Realizacja zadania będzie obejmowała 3 etapy: przeprowadzenie analizy literaturowej i opracowanie koncepcji rozwiązania, zaprojektowanie i realizację oraz weryfikację rozwiązania z analizą efektywności. Każdy etap zaliczany będzie na podstawie raportu. Istotne będzie prowadzenie dokumentacji projektu oraz przygotowanie prezentacji wyników projektu.

W drugiej grupie tematycznej projektów zespoły 2 osobowe będą badać odporność protokołów i mechanizmów komunikacyjnych w oparciu o ich analizę przy użyciu wybranego oprogramowania np. Nmap/Nessus/Wireshark/... Celem jest zapoznanie studentów z podstawami analizy komunikacji pakietowej oraz uświadomienie podstawowych zagrożeń wynikających z błędów projektowania protokołów.

ZAJĘCIA ZINTEGROWANE:
–

Treść kształcenia - streszczenie w jęz. angielskim:

The main objective of the course is to introduce students to the basics of system and application security. Aspects of hardware and software security will be discussed. The concepts of local and network cyberattack detection systems, attacks prevention methods and tools for security analysis and monitoring will be presented.

Egzamin: nie

Literatura i oprogramowanie:

Materiały do zajęć – slajdy, opracowania, artykuły

Książki:

1. A. J. White, B. Clark: *Blue Team Field Manual*; CreateSpace Independent Publishing Platform; ISBN 978-1541016361
2. B. Clark: *Red Team Field Manual*; CreateSpace Independent Publishing Platform; ISBN 978-1494295509
3. A. Harper et al.: *Gray Hat Hacking: The Ethical Hacker's Handbook*, 5th Ed.; McGraw-Hill Education; ISBN 978-1260108415
4. J. Luttgens, M. Pepe, K. Mandia: *Incident Response & Computer Forensics*, 3rd Ed.; McGraw-Hill Education; ISBN 978-0071798686
5. SP 800-61: *Computer Security Incident Handling Guide*; Rev.2; 2012; US NIST
6. C. Hadnagy: *Social Engineering: The Art of Human Hacking*; John Wiley & Sons; 1st edition, ISBN: 978-0470639535
7. Georgia Weidman: *Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne (Penetration Testing: A Hands-On Introduction to Hacking)*, ISBN: 978-83-283-0352-2, 9788328303522
8. Steve Suehring: *Zapory sieciowe w systemie Linux. Kompendium wiedzy o nftables. IV, (Linux Firewalls: Enhancing Security with nftables and Beyond (4th Edition*)), ISBN: 978-83-283-1297-5, 9788328312975
9. Peter Kim: *Bezpieczeństwo systemów informatycznych (The Hacker Playbook: Practical Guide To Penetration Testing)*, ISBN: 978-83-283-0384-3, 9788328303843
10. Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sébastien Josse: *Inżynieria odwrotna w praktyce. Narzędzia i techniki (Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation)*, ISBN: 978-83-283-0678-3, 9788328306783
11. William Stallings, Lawrie Brown: *Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1 (Computer Security: Principles and Practice (4th Edition), tom 1)*, ISBN: 978-83-283-4299-6, 9788328342996

Oprogramowanie:

1. Systemy operacyjne Windows, Linux – wersje klienckie i serwerowe;
2. Oprogramowanie open source i komercyjne do realizacji zadań praktycznych w ramach zajęć projektowych:
   - narzędzia do badać odporność protokołów i mechanizmów komunikacyjnych,

- narzędzia do emulacji systemów;
- narzędzia do monitoringu systemów, sieci i użytkowników;
- narzędzia do wykonywania aktywnych testów bezpieczeństwa systemów;

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	–	15

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia projektowe; w ramach tych zajęć student(ka), korzystając z oprogramowania (które jest dostępne w laboratorium, ale może być także zainstalowane na prywatnym komputerze studenta), wykorzystując podaną przez prowadzącego specyfikację problemu, opracowuje koncepcję realizacji, projektuje, przeprowadza weryfikację i optymalizację oraz wykonuje realizację systemu z wykorzystaniem dostępnych platform do prototypowania; student(ka) może ponadto uczestniczyć w prowadzonych co tydzień w wymiarze 1 godz. konsultacjach.

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocenę sprawozdań z realizacji projektu (poszczególnych etapów projektowych),
- ocenę wiedzy i umiejętności wykazanych na testach pisemnym o charakterze problemowym (w czasie testów student/ka może korzystać z dowolnych materiałów dydaktycznych oraz komputera),

Wymiar w jednostkach ECTS: 4 pkt.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. *liczba godzin kontaktowych – **50 godz.**, w tym*
   - *obecność na wykładach: **30 godz.**,*
   - *udział w konsultacjach związanych z realizacją projektu: **15 godz.** (zakładamy, że student korzysta z konsultacji dotyczących zainstalowania, uruchomienia i korzystania z oprogramowania, a ponadto z „regularnych" konsultacji 8 razy w semestrze),*
   - *udział w konsultacjach przedegzaminacyjnych: **2 godz.**,*
   - *obecność na egzaminie: **3 godz.** (pomijamy ew. egzamin ustny)*

2. *praca własna studenta – **55 godz.**, w tym*
   - *analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów i realizacji projektów: **15 godz.***
   - *realizacja projektu: **30 godz.** = 3 x 10 godz. (3 etapy: opracowanie koncepcji, projektowanie i optymalizacja, realizacja systemu na platformie docelowej i weryfikacja)*
   - *przygotowanie do testów: **10 godz.***

Łączny nakład pracy studenta wynosi 105 godz., **co odpowiada** 4 pkt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2 pkt. ECTS, co odpowiada 50 godz. kontaktowym.

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 2 pkt. ECTS (co odpowiada 55 godz. realizacji projektu)

Efekty kształcenia/uczenia się:

efekty kształcenia/uczenia się student, który zaliczył przedmiot:	forma zajęć/ technika kształcenia	sposób weryfikacji (oceny)*	odniesienie do efektów uczenia się dla programu
WIEDZA			
w1: ma wiedzę dotyczącą fundamentalnych pojęć z zakresu bezpieczeństwo systemów i oprogramowania	wykład + projekt	projekt, kololwium	W07 W09 W12
w2: ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu dotyczących bezpieczeństwa systemów	wykład + projekt	kololwium	W04 W07
w3: ma podstawową wiedzę z zakresu testów penetracyjnych	wykład	kololwium	W07
w4: ma podstawową wiedzę metodyki procesu zarządzania bezpieczeństwem systemów i oprogramowania	wykład + projekt	projekt, kololwium	W07 W08
w5: ma podstawową wiedzę z obszaru środków technicznych zapewniających bezpieczeństwo systemów i oprogramowania	wykład + projekt	projekt, kololwium	W07
w6: ma podstawową wiedzę z zakresu modelowania zagrożeń systemów i oprogramowania	wykład + projekt	projekt, kololwium	W07 W12
UMIEJĘTNOŚCI			
u1: potrafi przygotować środowisko pracy systemów i oprogramowania	wykład	projekt	U03
u2: potrafi wykorzystywać podstawowe narzędzia do przeprowadzenia testów bezpieczeństwa systemów i oprogramowania	wykład	projekt	U03
u3: potrafi modelować zagrożenia zgodnie z metodyką zarządzania jakością oprogramowania	wykład	projekt	U04 U07
u4: potrafi stosować środki techniczne zapewniające bezpieczeństwo sieci, systemów, oprogramowania i użytkowników	wykład	projekt	U08
u5: potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych	projekt	projekt	U09 U11
u6: potrafi przygotować i przeprowadzić prezentację dotyczącą zagadnień technicznych związanych z problemem rozwiązywanym na bieżąco	projekt	projekt	U10
u7: potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy	projekt	projekt	U01
KOMPETENCJE SPOŁECZNE			
ks1: ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	wykład + projekt	projekt	KS03 KS01
ks2: ma orientację zawodową w obszarze inżynierii systemów i oprogramowania i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze	wykład + projekt	projekt	KS03

Uwagi:

Wydziałowa Komisja Akredytacji Przedmiotów (WKAP)

–

Data i podpis autora (kierownika zespołu autorskiego):