Студијски програм: Мастер академске студије информатике

Назив предмета: НАПРЕДНЕ ТЕХНОЛОГИЈЕ У САЈБЕР БЕЗБЕДНОСТИ

Статус предмета: Изборни на свим модулима мастер академских студија информатике

Број ЕСПБ: 6

Услов: Уписан одговарајући семестар

Циљ предмета

Омогућити студентима стицање знања о безбедносним архитектурама заснованим на хардверској заштити и примени вештачке интелигенције за детекцију и превенцију сајбер напада. Посебан фокус је на Trusted Control Unit (TCU) архитектури фирме Axiado и zero-trust моделима.

Исход предмета

Након успешно савладаног предмета студент ће бити способан да: Разуме принципе root-of-trust и сигурног бутирања; Објасни архитектуру Axiado TCU чипа и његову улогу; Користи AI моделе за детекцију аномалија у системском понашању; Анализира zero-trust безбедносне архитектуре; Симулира нападе и развије основне AI детекторе за претње.

Садржај предмета

Теоријска настава

Хардверска безбедност: TPM, HSM, secure boot; Увод у детекцију напада помоћу AI модела; Axiado TCU чип – архитектура и употреба; Детекција претњи у реалном времену; Zero-trust приступ и његова имплементација; Безбедност у IoT и рбним уређајима;Open-source Trust решења – OpenTitan, TrenchBoot; Прикупљање и анализа системских логова; Симулација фирверских напада и детекција помоћу AI.

Практична настава

Упознавање са TPM2 симулатором и алатима за secure boot; Конфигурција и симулација secure boot процеса; Прикупљање системских логова (Linux, RPi); Коришћење AI за класификацију регуларног и нападног понашања; Тренинг AI модела за anomaly detection (Scikit-learn, Keras); Примена детектора на реалном систему (нпр. Raspberry Pi); Симулација brute-force и DoS напада; Увод у reverse engineering firmware-a (Ghidra, Binwalk); Студија случаја: анализа TCU архитектуре из Axiado докумената; Интеграција zero-trust модела на емулираном систему; Пројектни рад: AI безбедносни агент на рубном уређају; Припрема и презентација завршних пројеката.

Литература

1. Sarker, I. H., et al. (2024). *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation and Decision-Making*. Springer. ISBN 978-3031544965.
2. https://axiado.com/

Број часова активне наставе	**Теоријска настава:** **2**	**Практична настава:** **1 + 1**

Методе извођења наставе

Проблемски-оријентисана настава, практична настава, самостални рад студената, консултације. Комбинација класичне наставе са е-учењем и уз одговарајућу литературу.

Практична настава се обавља у виду лабораторијских вежби у рачунарским учионицама, на којима студенти самостално или уз помоћ асистената решавају реалне проблеме из области оптимизације.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	**70** поена	**Завршни испит**	**30** поена
колоквијуми	30	усмени испит	30
семинар-и	40		