BSK* 2020

Wprowadzenie, zasady zaliczania

O czym będą grupy z gwiazdką

Laboratoria będą podzielone na 4 mniej-więcej równe bloki:

- Aplikacje WWW
- Inżynieria wsteczna
- Eksploitacja programów binarnych
- Kryptografia

Każdemu z tych bloków odpowiada jedno zadanie zaliczeniowe.

Aplikacje WWW

O tym jak prawidłowo zabezpieczać aplikacje WWW i jakie błędy można popełnić, m.in.:

- SQL injection
- Same-origin policy, CSRF
- XSS
- CSP

Inżynieria wsteczna

O analizie działania programów binarnych, do których nie mamy źródeł

- Analiza statyczna: disasemblacja i dekompilacja kodu
- Analiza dynamiczna: śledzenie działania kodu w debuggerze

Eksploitacja programów binarnych

O błędach, jakie można popełnić pisząc w języku C (i podobnych) oraz tym, jak atakujący może je wykorzystać, by przejąć kontrolę nad naszym komputerem.

- Buffer overflow
- Integer overflow
- Use after free i inne błędy użycia sterty
- Eksploitacja: shellcode, ROP
- Zabezpieczenia przed eksploitacją: ASLR, NX, stack protector, ...

Kryptografia

Wprowadzenie do kryptografii i jej praktycznego użycia oraz błędy, jakie można popełnić implementując kryptografię:

- Czym jest szyfr blokowy, szyfr strumieniowy, funkcja skrótu, MAC, kryptografia asymetryczna
- Źródła losowości w praktyce
- Bezpieczne przechowywanie sekretów
- Timing attack

Zasady zaliczania

- Obowiązuje wspólny (ze zwykłym BSK) egzamin oraz zadanie z drzew ataku
- Zadania zaliczeniowe z BSK* zastępują pozostałe 6 zadań laboratoryjnych (24 punkty)
- Za każde zadanie można zdobyć 8 punktów, punktacja za laboratorium to min(z1+z2+z3+z4, 24) — można zdobyć maksymalną liczbę punktów oddając 3 zadania