Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodika k výučbe predmetu Reverzné inžinierstvo a analýza malvéru

v rámci magisterského študijného programu Aplikovaná informatika

(aktivita A2 – Tvorba metodík a vzdelávacích materiálov pre účely vzdelávania v oblasti kybernetickej a informačnej bezpečnosti)

Košice, marec 2026

Názov predmetu: Reverzné inžinierstvo a analýza malvéru
Kód predmetu:

Krátka anotácia predmetu:

Predmet sa zameriava na systematický proces reverzného inžinierstva a analýzy malvéru, ktorého cieľom je odhaliť vnútornú architektúru, logiku a funkčnosť softvéru aj bez prístupu k pôvodnému zdrojovému kódu. Študenti sa postupne oboznámia so statickou analýzou, ktorá zahŕňa prácu s asemblérom či nástrojmi ako Ghidra, a následne aj s dynamickou analýzou na pozorovanie správania škodlivého kódu v kontrolovanom prostredí (sandbox). Dôležitou súčasťou kurzu je hĺbkové skúmanie operačných systémov Linux a Windows, ich pamäťových štruktúr, API volaní a binárnych formátov ELF a PE.. Pozornosť sa venuje aj pokročilým technikám, ktoré malvér používa na svoje ukrytie a sťaženie analýzy, ako sú polymorfizmus, obfuskácia, injektáž kódu do iných procesov či anti-debugovacie mechanizmy. Ďalším dôležitým blokom je bezpečnosť IoT zariadení a reverzné inžinierstvo firmvéru vo vnorených systémoch s ohľadom na špecifické architektúry ako ARM. Jednotlivé prednášky sú postavené spôsobom poskytovania nových faktov pričom sa dôležité aspekty matérie opakujú a postupne rozvíjajú s cieľom zabezpečiť komplexné pochopenie problematiky reverzného inžinierstva a analýzy malvéru zo strany študentov.

Cieľová skupina:

Študenti magisterského štúdia programov informatiky a aplikovanej informatiky.

Ciele vzdelávania

- **Pochopenie transformácie kódu:** Pochopiť, ako sa logika z vyšších programovacích jazykov (napríklad C) transformuje do nízkoúrovňového asembléru, špecificky pri kompilácii (napr. GCC na Linuxe).
- **Identifikácia skrytých mechanizmov:** Naučiť sa v strojovom kóde identifikovať kryptografické rutiny a iné skryté funkcie.
- **Analýza obranných techník malvéru:** Schopnosť analyzovať a prekonávať pokročilé techniky, ktoré malvér využíva na svoje ukrytie a sťaženie analýzy, ako sú obfuskácia, anti-debugging a anti-VM (anti-virtualizačné) mechanizmy.
- **Osvojenie si "dirty hands" prístupu a nízkoúrovňových princípov:** Naučiť študentov syntetizovať znalosti o interných štruktúrach jadra operačných systémov, architektúre procesorov a binárnych formátoch (ako sú ELF a PE), keďže spoliehať sa len na automatizované GUI nástroje pre modernú analýzu hrozieb nestačí.
- **Zlepšenie zručností v hybridnej analýze:** Zvládnuť kombinovanie statickej analýzy (napr. v nástroji Ghidra pre získanie prehľadu o štruktúre) s dynamickou analýzou (napr.

ladenie pomocou Fridy pre sledovanie reálneho správania kódu a dešifrovanie kontextu v izolovanom prostredí).

- **Skúmanie moderných a špecifických hrozieb:** Získať zručnosti pre reverzné inžinierstvo a emuláciu firmvéru IoT a embedded zariadení a oboznámiť sa s modernými technikami útokov, ako sú eBPF rootkity či bezsúborový (fileless) malvér.

Stručná osnova predmetu:

1. Úvod do štúdia reverzného inžinierstva a analýzy malvéru.
2. Analýza architektúry pamäte a exploitácia binárnych zraniteľností.
3. Základné aspekty nízkoúrovňového jazyka (asembler) a nízkoúrovňová analýza strojového kódu.
4. Prevod strojového kódu na inštrukcie a zdrojový kód — disassembling a dekompilácia.
5. Dynamická analýza strojového kódu a správania programov.
6. Pokročilá analýza kódu a dynamické ladenie strojového kódu.
7. Rozšírené techniky reverzného inžinierstva v operačnom systéme Linux.
8. Rozšírené techniky analýzy malvéru v prostredí operačného systému Linux.
9. Základy reverznej analýzy kódu v OS Windows.
10. Pokročilé techniky reverznej analýzy kódu a analýzy malvéru v operačnom systéme Windows.
11. Získavanie firmvéru jednoúčelových zariadení a jeho analýza.
12. Pokročilá reverzná analýza firmvéru jednoúčelových zariadení

Odporúčaná literatúra:

1. SIKORSKI, Michael — HONIG, Andrew. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco : No Starch Press, 2012.
2. EAGLE, Chris — NANCE, Kara. The Ghidra Book: The Definitive Guide. San Francisco : No Starch Press, 2020.
3. DENNIS, Andriesse. Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. San Francisco : No Starch Press, 2019.
4. HALE LIGH, Michael — CASE, Andrew — LEVY, Jamie — WALTERS, Aaron. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis : Wiley, 2014.
5. SVAJCER, Vanja. Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks. 2nd ed. Birmingham : Packt Publishing, 2022.
6. CHEN, Aditya — ZADDACH, Jonas — COSTIN, Andrei. Firmware Security: Vulnerabilities, Exploits, and Best Practices for IoT Devices. Hoboken : Wiley, 2025.

<u>Akademické a výskumné platformy</u>

1. MITRE ATT&CK Framework: https://attack.mitre.org/
2. MITRE CWE (Common Weakness Enumeration): https://cwe.mitre.org/
3. VirusTotal: https://www.virustotal.com/

Vyučujúci:

Poznámky:

Detailná osnova predmetu

Prednáška 1: Úvod do štúdia reverzného inžinierstva a analýzy malvéru

- definícia reverzného inžinierstva a jeho základné charakteristiky
- definícia základných pojmov
- typológia bezpečnostných hrozieb
- návrh bezpečného laboratória

Prednáška 2: Analýza architektúry pamäte a exploitácia binárnych zraniteľností

- charakteristika a štruktúra počítačovej pamäte
- ukazovateľ na pamäť v programe v jazyku C
- dynamická alokácia pamäte
- typické programátorské chyby pri práci s pamäťou v jazyku C

Prednáška 3: Základné aspekty nízkoúrovňového jazyka (asembler) a nízkoúrovňová analýza strojového kódu

- definícia počítačovej architektúry
- procesor a registre
- Asemblér a konvencia volania systémových volaní
- úvod do exploitácie

Prednáška 4: Prevod strojového kódu na inštrukcie a zdrojový kód — disassembling a dekompilácia

- anatómia ELF súboru (Linux)
- pamäť - rôzne pohľady na štruktúrovanie pamäte (sekcia, segmenty)
- algoritmy disassemblovania
- dekompilácia a dostupné nástroje

Prednáška 5: Dynamická analýza strojového kódu a správania programov

- statická vs. dynamická analýza binárneho spustiteľného súboru
- architektúra bezpečného prostredia vhodného na dynamickú analýzu

- nástroje vhodné na dynamickú analýzu procesov
- úvod do techník využívaných škodlivým softvérom

Prednáška 6: Pokročilá analýza kódu a dynamické ladenie strojového kódu

- definícia paradigmy ladenia (debuging)
- ladiace rozhrania a nástroje
- anti-debugging techniky škodlivého softvéru
- úvod do techniky "dátového zahmlievania" (obfuskácia)

Prednáška 7: Rozšírené techniky reverzného inžinierstva v operačnom systéme Linux

- kontext a evolúcia hrozieb v operačnom systéme Linux
- pokročilé techniky analýzy "dátového zahmlievania"
- pokročilé techniky reverznej analýzy a eBPF
- forenzná rekonštrukcia dátových artefaktov

Prednáška 8: Rozšírené techniky analýzy malvéru v prostredí operačného systému Linux

- možnosti interakcie a šírenia škodlivého softvéru
- detailný pohľad na polymorfizmus a metamorfizmus
- dekódovanie a dešifrovanie vzoriek škodlivého softvéru
- extrakcia šifrovacích kľúčov

Prednáška 9: Základy reverznej analýzy kódu v OS Windows

- architektúra operačného systému Windows
- definícia a analýza formátu spustiteľných súborov
- Windows API a využívanie dynamických knižníc
- statická a dynamická analýza v prostredí OS Windows, pamäťová forenzná analýza

Prednáška 10: Pokročilé techniky reverznej analýzy kódu a analýzy malvéru v operačnom systéme Windows

- detailný pohľad na manažment procesov
- techniky škodlivého softvéru: injektáž kódu, perzistencia, eskalácia privilégií
- detekčné techniky škodlivého softvéru a techniky "dátového zahmlievania"
- nástroje pre pokročilú analýzu

Prednáška 11: Získavanie firmvéru jednoúčelových zariadení a jeho analýza

- definícia a analýza pamäťových médií jednoúčelových zariadení

- neinvazívna a invazívna extrakcia firmvéru
- Špecifikácia architektúr jednoúčelových zariadení
- úvod do súborových systémov

Prednáška 12: Pokročilá reverzná analýza firmvéru jednoúčelových zariadení

- analýza bezpečnostnej úrovne jednoúčelových zariadení
- statická analýza a detailný pohľad na špecializované súborové systémy
- dynamická analýza a koncept “re-hostingu” firmvéru (emulácia)
- hybridná analýza firmvéru

Podmienky hodnotenia

Forma ukončenia: klasifikované hodnotenie.

Záverečná skúška.