

Анализ программного кода

Введение

доц. Нестеренко В.А.

Цель и содержание курса

Знакомство с основными принципами и деталями размещения и исполнения программного кода на персональном компьютере с целью его анализа, улучшения и защиты.

Задачи:

- знакомство с общими принципами разбора анализа программного кода как в виде исходных текстов так и в виде исполнимых модулей;
- изучение основных инструментов анализа исполнимых программных модулей (отладчик, дизассемблер, профайлер, ...);
- изучение методов выявления подозрительных и вредоносных участков кода и изучение возможности защиты программ от средств анализа.

Исполнение кода

код операции	← адрес
операнды	
	1. Читает адрес из программного счётчика
код операции	2. По коду операции определяет размер команды
операнды	3. Вычисляет адрес следующей команды
	4. Записывает полученный адрес в программный счётчик
...	
...	
...	5. Выполняет текущую команду
...	6. Переходит к шагу 1

Регистры процессора

Регистры – основное (единственное) средство общения программы с процессором.

Обращение к регистрам по имени (не по адресу как в случае с ячейками памяти).

Группы регистров:

- *Регистры общего назначения (РОН)* используются для хранения и модификации данных и адресов.
- *Сегментные регистры* используются для работы с памятью.
- *Регистры состояния и управления* содержат информацию о состоянии процессора и исполняемой команде программы.

Регистры общего назначения

EAX, EBX, ECX, EDX

32	16	8	
EAX (EBX, ECX, EDX)			
		AX (BX, CX, DX)	
		AH	AL

ESI, EDI, EBP, ESP

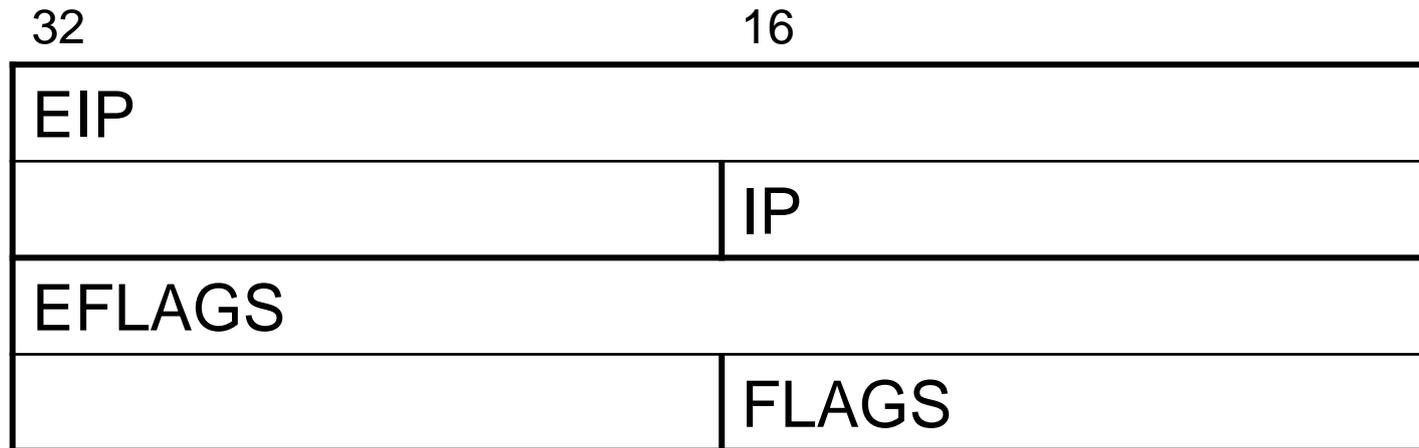
32	16
ESI (EDI, EBP, ESP)	
	SI (DI, BP, SP)

Сегментные регистры

16

CS – команды
SS – стек
DS – данные
ES – данные
FS – данные
GS – данные

Регистры состояния и управления



Модель память

**Адресное
пространство
программы**



**Физическое
адресное
пространство**

Линейная модель
Сегментная модель
Страничная модель

Машинный код, Язык Ассемблера

...