Операционные системы

Лекция 7

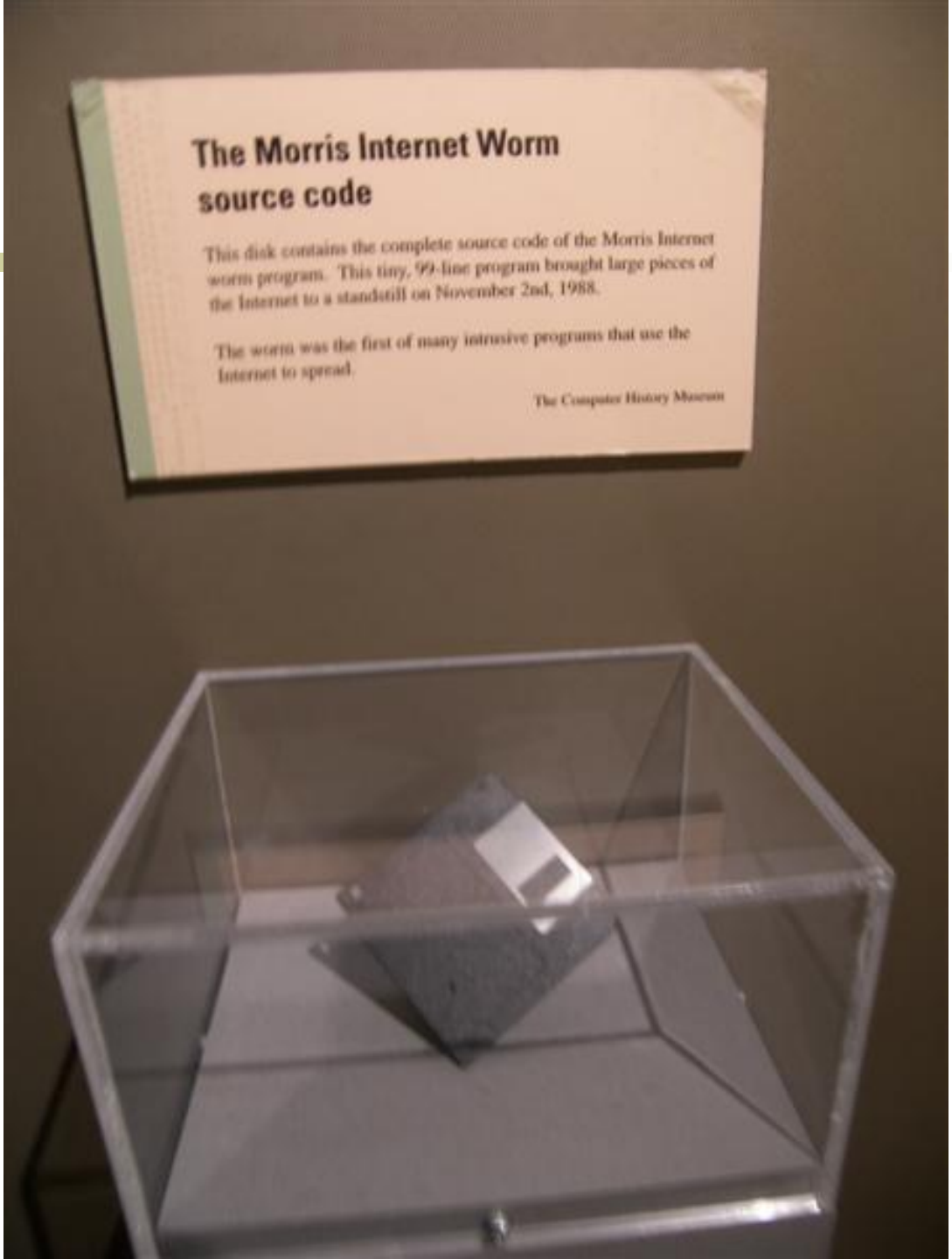
Основы безопасности ОС

Контрольные вопросы

- Алгоритмы чтения информации с жесткого диска?
- Опишите принцип адресации файлов в ФС FAT32.
- Опишите структуру и функции MFT в ФС NTFS. Какие типы атрибутов файлов поддерживает NTFS?
- Опишите принцип адресации файлов в UNIX V.
- Сравните назначение прав доступа в ФС FAT32, NTFS и UNIX V FS.
- Каким образом реализована поддержка длинных имен файлов в VFAT?
- Какие ограничения существуют на загрузочный раздел WinNT и почему?

Контрольные вопросы

- Принцип локальности
- Методы организации памяти
- Адресация памяти при сегментно-страничной структуре
- Методы предотвращения тупиков


The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
The Computer History Museum

Типы вирусов

- Viruses
  - Resident
  - Non-resident
- Trojans
- Macros
- Cross-site scripting

Угрозы безопасности

- confidentiality
- availability
- Integrity

- Активные
- Пассивные

- Проникновение
- Несанкционированные действия
- Вредоносное ПО

Orange book

- D — Minimal Protection
- C — Discretionary Protection
- C1 — Discretionary Security Protection
- C2 — Controlled Access Protection
- B — Mandatory Protection
- B1 — Labeled Security Protection
- B2 — Structured Protection
- B3 — Security Domains
- A — Verified Protection
- A1 — Verified Design

Рекомендации для проектирования системы безопасности

- Проектирование системы должно быть открытым.
- Не должно быть доступа по умолчанию.
- Нужно тщательно проверять текущее авторство.
- Давать каждому процессу минимум возможных привилегий.
- Защитные механизмы должны быть просты, постоянны и встроены в нижний слой системы, это не аддитивные добавки.
- Важна физиологическая приемлемость.

Криптография

- Методы шифрования с секретным или симметричным ключом (DES, TripleDES)
- Методы шифрования с открытым или асимметричным ключом (RSA)

Аутентификация

- CHAP (Challenge Handshake Authentication Protocol)

Авторизация

- способы управления доступом:
  - дискреционный (избирательный)
  - полномочный (мандатный).

Объект / Домен	F1	F2	F3	Printer
D1	read			
D2				print
D3		read	execute	
D4	read write		read write	

Матрица доступа

- Список прав доступа. Access control list
- Мандаты возможностей. Capability list

- lock-key

Выявление вторжений

- Аудит
  - вход или выход из системы;
  - операции с файлами (открыть, закрыть, переименовать, удалить);
  - обращение к удаленной системе;
  - смена привилегий или иных атрибутов безопасности.
- Сканирование
  - короткие или легкие пароли;
  - неавторизованные set-uid программы;
  - неавторизованные программы в системных директориях;
  - долго выполняющиеся программы;
  - нелогичная защита как пользовательских, так и системных директорий и файлов;
  - потенциально опасные списки поиска файлов;
  - изменения в системных программах.

Анализ некоторых популярных ОС

- MS DOS
- NetWare
- OS/2
- UNIX
- Windows NT
  - Local Security Authority, LSA
  - Security Account Manager, SAM
  - Security Reference Monitor, SRM

Философия и архитектура NT против UNIX с точки зрения безопасности

Windows vs UNIX

- Open Source vs дизассемблер
- Удаленный доступ
- Комплектность штатной поставки
- Механизмы аутентификации
- Повышение своих привилегий
- Угроза переполнения буфера
- Доступ к чужому адресному пространству
- Межпроцессорные коммуникации

Windows vs UNIX

характеристика	NT	UNIX
качество и полнота документирования	документирована поверхностно	документирована весьма обстоятельно
доступность исходных текстов	исходные тексты недоступны	исходные тексты доступны

Windows vs UNIX

характеристика	NT	UNIX
сложность анализа	высокая	умеренная
распространенность	существует весьма ограниченное количество представителей NT, причем наблюдается ярко выраженная преемственность дыр от одних версий системы к другим	существует огромное количество разнообразных клонов, причем ошибки одной версии системы зачастую отсутствуют в остальных

Windows vs UNIX

характеристика	NT	UNIX
сложность кода	код излишне сложен	код предельно прост
поддержка удаленного администрирования	частично поддерживает	поддерживает

Windows vs UNIX

характеристика	NT	UNIX
комплектность штатной поставки	содержит минимум необходимых приложений	содержит огромное количество приложений, в том числе и не протестированных
механизмы аутентификации	устойчив к перехвату паролей	передает открытый пароль

Windows vs UNIX

характеристика	NT	UNIX
использование привязки	не использует	использует
выполнение привилегированных операций	выполняется операционной системой	выполняется самим приложением со временным повышением привилегий

Windows vs UNIX

характеристика	NT	UNIX
модель пользователей	иерархическая	одноуровневая
защита от переполнения буфера	отсутствует, причем сама ОС написана на языке, провоцирующем такие ошибки	отсутствует, причем сама ОС написана на языке, провоцирующем такие ошибки

Windows vs UNIX

характеристика	NT	UNIX
возможность доступа в адресное пространство чужого процесса	имеется, разрешена по умолчанию	отсутствует
возможность отладки процессов	имеется, разрешена по умолчанию	имеется, но связана с рядом ограничений

Windows vs UNIX

характеристика	NT	UNIX
возможность отладки активных процессов	имеется, но требует наличия соответствующих привилегий	отсутствует
удаленный доступ к именованным каналам	есть	нет

Windows vs UNIX

характеристика	NT	UNIX
создание подложных именованных каналов	есть, можно создать и канал, и даже подложный экземпляр уже открытого канала	есть, можно создать лишь подложный канал
защита именованных каналов от нежелательных подключений	отсутствует	отсутствует

Windows vs UNIX

характеристика	NT	UNIX
защита сокетов от нежелательных подключений	отсутствует	отсутствует
возможность эмуляции ввода в более привилегированный процесс	имеется	отсутствует

Вопросы?