Безопасность уровня операционных систем

LOGO

Виды “дыр” в компьютерной сети

Типы дыр в операционной системе Windows:

Удаление информации, случайно оставшейся на свободном месте вашего жесткого диска, не может удалить ту конфиденциальную информацию, которая была помещена ОС Windows в части других файлов;

Удаление концов файлов не может надежно удалить ту информацию, которая оказалась записанной внутри файлов, создаваемых такими программами, как Word Excel.

Известная всем многозадачность ОС Windows, которая позволяет одновременно выполнять несколько программ, может выдать вашим врагам конфиденциальные документы, пароли и даже шифровальные ключи;

Каждый раз при распечатке очередного документа ОС Windows оставит на жестком диске незашифрованную копию этого документа несмотря на то, что вы тщательно зашифровали свою копию. Многие программы, с которыми вы работаете, также оставляют после своей работы копии конфиденциальной информации во временных директориях;

Файловая система ОС Windows может игнорировать команду, полученную от криптографической программы, которая требует переписать случайными данными то место на диске компьютера, где размещались копии конфиденциальных файлов, после того, как файлы были зашифрованы и должны были быть надежно удалены (переписаны случайными данными). В результате, конфиденциальная информация может остаться на вашем жестком диске в открытом виде несмотря на то, что вы дали команду уничтожить файлы с информацией через интерфейс криптографической программы;

7 наиболее распространенных угроз

- Угроза 1. Физические атаки
- Угроза 2. Кража паролей
- Угроза 3. Назойливое сетевое соседство
- Угроза 4. Вирусы, черви и другие «враждебные» программы
- Угроза 5. Внешние «враги» и создатели троянских коней
- Угроза 6. Вторжение в сферу частных интересов
- Угроза 7. Фактор электронной почты

Задачи системы безопасности Windows NT

- Управление доступом
- Контроль
- Безопасность хранения данных

Процесс авторизации

- Процесс ввода в систему (logon processes)
- Распорядитель локальной безопасности (local security authority, LSA)
- Диспетчер бюджетов безопасности (Security Accounts Monitor, SAM)
- Монитор безопасности (Security Reference Monitor, SRM)

Процесс ввода в систему

Регистрация пользователей

- **Идентификация**
- **Аутентификация**
- **Авторизация**

Авторизация –

процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

идентификатор которого он использует.

LSA

- **Сервер проверки подлинности локальной системы безопасности (англ. *Local Security Authority Subsystem Service*, LSASS) — часть операционной системы *Windows*, отвечающая за авторизацию локальных пользователей отдельного компьютера. Сервис является критическим, так как без него вход в систему для локальных пользователей (не зарегистрированных в домене) невозможен в принципе.**
- **Процесс проверяет данные для авторизации, при успешной авторизации служба выставляет флаг о возможности входа. Если авторизация была запущена пользователем, то также ставится флаг запуска пользовательской оболочки. Если авторизация была инициализирована службой или приложением, данному приложению предоставляются права данного пользователя.**

SAM

SAM (англ. *Security Account Manager*) Диспетчер учётных записей безопасности — RPC-сервер Windows, оперирующий базой данных учетных записей.

SAM выполняет следующие задачи:

- **Идентификация субъектов (трансляции имен в идентификаторы (SID'ы) и обратно);**
- **Проверка пароля, авторизация (участвует в процессе входа пользователей в систему);**
- **Хранит статистику (время последнего входа, количества входов, количества некорректных вводов пароля);**
- **Хранит настройки политики учетных записей и приводит их в действие (политика паролей и политика блокировки учетной записи);**
- **Хранит логическую структуру группировки учетных записей (по группам, доменам, алиасам);**

SAM

- Контролирует доступ к базе учетных записей;
- Предоставляет программный интерфейс для управления базой учетных записей.

База данных SAM хранится в реестре (в ключе HKEY_LOCAL_MACHINE\SAM\SAM), доступ к которому запрещен по умолчанию даже администраторам.

SAM-сервер реализован в виде DLL-библиотеки samsrv.dll, загружаемой lsass.exe. Программный интерфейс для доступа клиентов к серверу реализован в виде функций, содержащихся в DLL-библиотеке samlib.dll.

Объектная модель защиты

ACL

Дескрипторы безопасности (SD, Security Descriptor)

DACL англ. *Discretionary Access Control List*

SACL англ. *System Access Control List*

Active Directory (активные директории Windows NT (1999 г), реализация службы каталогов NT Directory Service, NTDS)

Encrypting File System (EFS) – система шифрования файлов

Дескрипторы безопасности

- Каждому контейнеру и объекту в сети назначается набор данных, относящихся к управлению доступом. Этот набор данных, называемый дескриптором безопасности, определяет, какой тип доступа разрешается пользователям и группам. Дескриптор безопасности создается автоматически вместе с контейнером или объектом. Типичным примером объекта с дескриптором безопасности является файл.

Дескрипторы безопасности

- Разрешения определяются в дескрипторе безопасности объекта. Разрешения сопоставляются, или назначаются, конкретным пользователям или группам. Например, группе «Администраторы» могут быть назначены разрешения на чтение, запись и удаление файла Temp.dat, а группе «Операторы» — только на его чтение и запись.
- Каждое назначение разрешений пользователю или группе называется элементом разрешения, который является видом записи управления доступом (ACE). Весь комплект элементов разрешений в дескрипторе безопасности называется набором разрешений, или таблицей управления доступом (ACL). Так, набор разрешений для файла Temp.dat включает два элемента: один для группы «Администраторы», другой для группы «Операторы».

DACL и SACL

- Списки DACL обеспечивают программное управление доступом к защищенным ресурсам, в то время как списки SACL обеспечивают программное управление политиками аудита системы для защищенных ресурсов.
- Например, с помощью DACL можно обеспечить возможность чтения файла только администратором; с помощью SACL можно обеспечить запись в журнал всех успешных попыток открытия файла.

DACL

- **DACL, англ. *Discretionary Access Control List* — список избирательного управления доступом, контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом (чтение, запись, удаление и т. д.)**

SACL

- SACL, англ. *System Access Control List* — список управления доступом к объектам Microsoft Windows, используемый для аудита доступа к объекту.
- SACL - это традиционный механизм логирования событий, который определяет, как проверяется доступ к файлам и папкам. В отличие от DACL, SACL не может ограничивать доступ к файлам и папкам. Но он может отследить событие, которое будет записано в журнал событий безопасности(security event log), когда пользователь обратится к файлу или папке. Это отслеживание может быть полезно при решении проблем доступа или при определении запрещенного проникновения.

Active Directory

Active Directory («Активный каталог», *AD*) — LDAP) — LDAP-совместимая реализация службы каталогов) — LDAP-совместимая реализация службы каталогов корпорации Microsoft) — LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server) — LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Позволяет администраторам использовать групповые политики) — LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение) — LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Позволяет

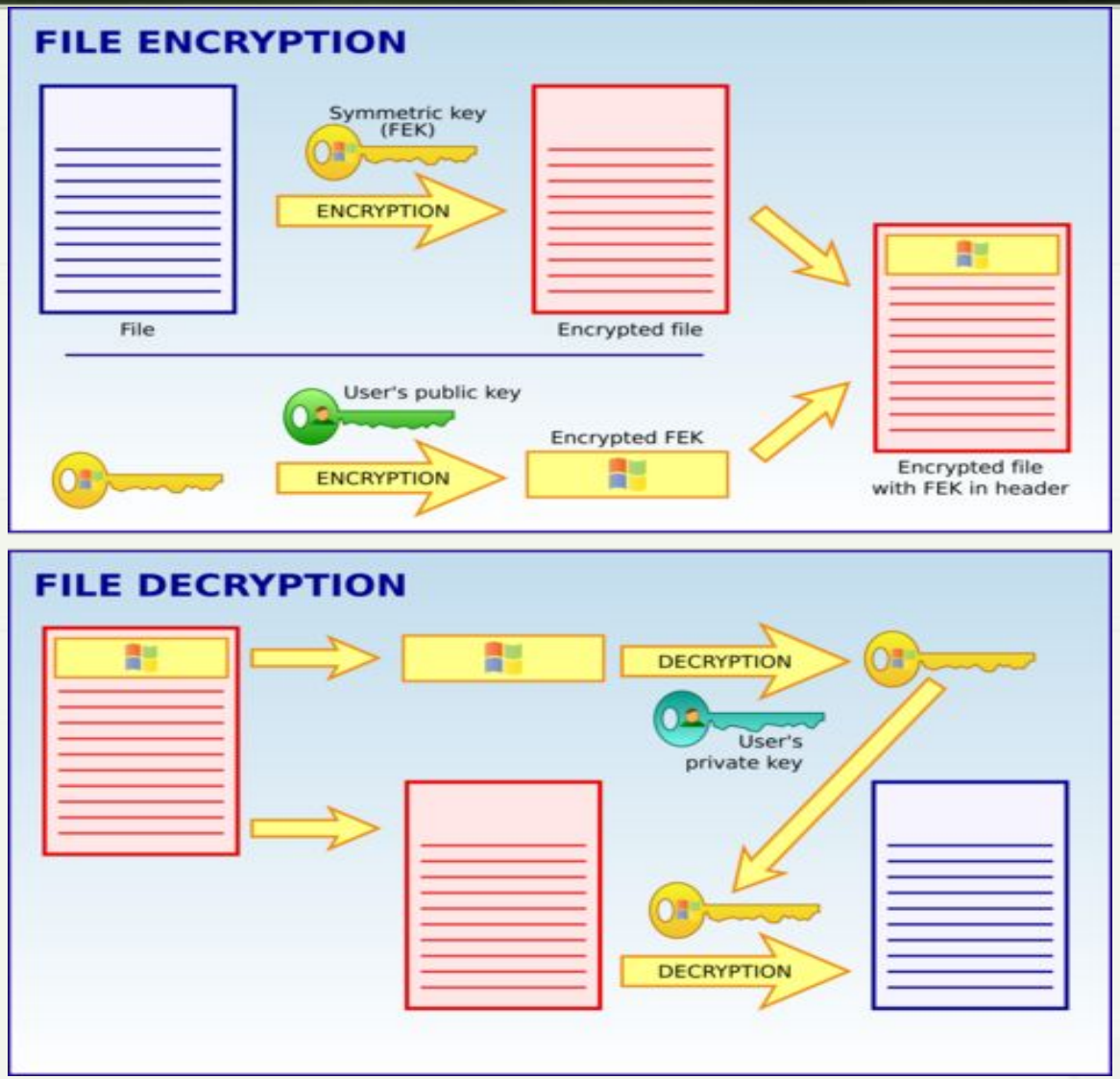
Система шифрования файлов (EFS)

Encrypting File System (EFS) — система шифрования данныхEncrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NTEncrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NT (начиная с Windows 2000Encrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NT (начиная с Windows 2000 и выше), за исключением «домашних» версий (Windows XP Home EditionEncrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных

Система шифрования файлов (EFS)

Аутентификация пользователя и права доступа к ресурсам, имеющие место в NT, работают, когда операционная система загружена, но при физическом доступе к системе возможно загрузить другую ОС, чтобы обойти эти ограничения. EFS использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре открытый/закрытый ключ для защиты случайно сгенерированного ключа шифрования для каждого файла. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, и защищённость данных зависит от стойкости пароля пользователя.

Система шифрования файлов (EFS)



Алгоритм шифрования/расшифрования файлов

Управление доступом к объектам

Использование файловой системы NTFS

NTFS

- **NTFS — стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft.**
- **NTFS поддерживает разграничение доступа к данным для различных пользователей и групп пользователей (списки контроля доступа — англ. *access control lists*, ACL), а также позволяет назначать дисковые квоты (ограничения на максимальный объём дискового пространства, занимаемый файлами тех или иных пользователей)**

Уровень защищённости C2

Основные требования:

Владелец ресурса (например, файла) должен иметь возможность управлять доступом к ресурсу.

Операционная система должна защищать объекты от несанкционированного использования другими процессами. Например, система должна защищать память так, чтобы ее содержимое не могло читаться после освобождения процессом, и после удаления файла не допускать обращения к данным файла.

Перед получением доступа к системе каждый пользователь должен идентифицировать себя, вводя уникальное имя входа в систему и пароль. Система должна быть способна использовать эту уникальную идентификацию для контроля действий пользователя.

Администратор системы должен иметь возможность контроля связанных с безопасностью событий (audit security-related events). Доступ к этим контрольным данным должен быть ограничен администратором.

Система должна защищать себя от внешнего вмешательства типа модификации выполняющейся системы или хранимых на диске системных файлов.

Модель безопасности Windows 2000

Протокол Kerberos

- модель непрямой аутентификации
- может использовать централизованное хранение аутентификационных данных и является основой для построения механизмов (Single Sign-On)
- механизм взаимной аутентификации клиента и сервера перед установлением связи между ними
- протокол основан на понятии ticket, который является зашифрованным пакетом данных, выданным центром аутентификации
- впервые применен в ОС Windows 2000

Основные новшества в системе безопасности Windows 2000

Улучшение средств аутентификации в сети:

- Аутентификация Kerberos
- Применение сертификатов
- Поддержка смарт-карт

Безопасность хранения данных:

- Файловая система NTFS
- Шифрующая файловая система
- Квотирование дисков
- Контроль изменений

Сетевая безопасность

- Возможность шифрования данных, передаваемых по сети IPsec
- Фильтрация пакетов IP
- Поддержка VPN

Стратегия безопасности Windows XP

- Аутентификация
- Авторизация
- Группы безопасности
- Политика групп
- Шифрование

  - Администраторы (Administrators)
  - Опытные пользователи (Power Users)
  - Пользователи (Users)
  - Гости (Guests)

Ограничение на учетные записи с пустыми паролями в Windows XP

Для безопасности пользователей, не защитивших свою учетную запись паролем, в Windows XP Professional такие учетные записи разрешено применять только для входа в систему компьютера с его консоли.

Шифрованная файловая система (Encrypting File System, **EFS**)

Шифрование базы данных автономных файлов

Управляемый доступ к сети в Windows XP

Windows XP содержит встроенную подсистему безопасности для предотвращения вторжений. Ее работа базируется на ограничении прав любого, кто пытается получить доступ к компьютеру из сети до привилегий гостевой учетной записи.

В Windows XP Professional по умолчанию все пользователи, вошедшие по сети, работают под учетной записью Guest. Это исключает для злоумышленника возможность войти в систему через Интернет под локальной учетной записью Администратор (Administrator), у которой нет пароля.

Упрощенное совместное использование ресурсов в Windows XP

Модель совместного использования и безопасности для локальных учетных записей позволяет выбрать модель безопасности на основе применения исключительно гостевой учетной записи (Guest) либо классическую (Classic) модель безопасности.

В гостевой модели при любых попытках войти в систему локального компьютера через сеть применяется только гостевая учетная запись.

В классической модели пользователи при доступе через сеть входят в систему локального компьютера под своими учетными записями.

На компьютерах в составе домена эта политика не применяется, а по умолчанию используется гостевая учетная запись.

Корпоративная безопасность Windows XP

В Windows XP имеются предопределенные шаблоны безопасности, обычно используемые без изменений или как основа для особой настройки конфигурации безопасности.

Эти шаблоны безопасности применяются при:

создании ресурса, такого как общая папка или файл;

при этом вы вправе воспользоваться заданными по умолчанию ACL или настроить их в соответствии со своими потребностями

распределении пользователей по стандартным группам безопасности,

таким как Users, Power Users и Administrators, **и принятии заданных по умолчанию параметров ACL**

использовании предоставляемых ОС шаблонов групповой политики –

Basic (основной), Compatible (совместимый), Secure (безопасный) или Highly Secure (высокобезопасный)

Службы сертификации Windows XP

Службы сертификации - это компонент базовой ОС, позволяющий ей выполнять функции центра сертификации (certification authority, CA), или ЦС, в том числе выпускать цифровые сертификаты и управлять ими.

- Хранилище сертификатов с открытыми ключами
- Хранение закрытых ключей
- Автоматический запрос сертификата пользователя
- Запросы в ожидании и обновление сертификатов

Личная конфиденциальность в Windows XP

Возможности обеспечения личной конфиденциальности в Windows XP Professional такие же, как и в Windows XP Home Edition. Они различаются при работе в домене или в составе рабочей группы и в изолированном режиме. В домене применяется назначенная администратором политика.

Доступ к Интернету – Internet Connection Firewall

Межсетевой экран Internet Connection Firewall в Windows XP Professional обеспечивает защиту настольных и переносных компьютеров при подключении к Интернету - особенно в случае постоянных подключений, таких как кабельные модемы и DSL.

Параметры групповой политики, относящиеся к безопасности

Существуют определенные политики управления паролем:

-определение минимальной длины пароля
-настройка интервала между обязательной сменой пароля
-управление доступом к ресурсам и данным

Политика ограничения используемых приложений в Windows XP

Эта политика предоставляет администраторам механизм определения и управления ПО, работающим в домене. Она позволяет ограничить круг приложений только разрешенным к выполнению ПО и запрещает работу нежелательных приложений, среди которых вирусы и "троянцы", а также другое ПО, вызывающее конфликты.

Политика ограничения применяется и на изолированных компьютерах при конфигурировании политики локальной защиты. Она также интегрируется с групповой политикой и Active Directory. Можно задать разные политики ограничения используемых приложений для различных подмножеств пользователей или компьютеров.

Протокол IPSec в Windows XP

Безопасность IP-сетей - почти стандартное требование в нынешнем деловом мире с Интернетом, интрасетями, отделениями и удаленным доступом. Поскольку конфиденциальная информация постоянно пересылается по сети, сетевые администраторы и другие специалисты службы поддержки должны обеспечить защиту этого трафика от:

- изменения данных при пересылке
- перехвата, просмотра и копирования
- несанкционированного олицетворения определенных ролей
- перехвата и повторного использования для получения доступа к конфиденциальным ресурсам

Поддержка смарт-карт в Windows XP

Смарт-карта - это устройство с интегральной схемой, предназначенное для безопасного хранения открытых и закрытых ключей, паролей и прочей личной информации. Она служит для операций шифрования с открытым ключом, проверки подлинности, введения цифровой подписи и обмена ключами.

Смарт-карта представляет собой следующие функции:

- особо защищенное хранилище для закрытых ключей и другой частной информации;
- изоляцию чрезвычайно важных для безопасности вычислений, в том числе проверки подлинности, цифровой подписи и обмена ключами, от других компонентов системы, которые напрямую не работают с этими данными;
- свободу перемещения реквизитов пользователей и другой частной информации между компьютерами на работе и дома, а также удаленными компьютерами

Как защитить себя?

Формирование всестороннего плана по поддержке мер безопасности:

- Своевременная установка патчей
- Обеспечение физической защиты
- Применение замысловатых паролей
- Установка антивирусного программного обеспечения
- Использование программ-брандмауэров
- Резервное копирование данных