Безопасность

Операционные системы 2011/12

Татьяна Романова

17 декабря 2011 г.

План на сегодня

- Безопасность и угрозы для нее
- Шифрование и подписи
- Аутентификация
- Атаки изнутри системы
- Известные примеры
- Вирусы и антивирусы

Материалы

- Э. Таненбаум, Соверменные операционные системы, глава 9.
- CS 162, лекция 25, 26 (видео лекции на YouTube).

Безопасность и механизмы защиты

Механизмы защиты — средства для контроля доступа

- процессов к ресурсам (например, механизм виртуальных адресов, обеспечивает защиту страниц памяти)
- пользователей к данным (права доступа к файлам)

Возможные угрозы:

- распространение конфиденциальных данных
- порча или подделка данных
- отказ в обслуживании

Кто виноват?

- Злоумышленники:
  - Случайные любопытные пользователи (читают чужие сообщения, открытые на чтение чужие файлы и т. п.)
  - Just for fun: студенты, взламывающие сервер или пишущие вирус просто потому, что можно.
  - Желающие личного обогащения (взлом банковских систем, шантаж).
  - Занимающиеся промышленным или военным шпионажем
- Случайная потеря данных:
  - Форс-мажор (пожары, наводнения, войны)
  - Аппаратные и программные ошибки (сбой процессора, ошибки в оперативной памяти, нечитаемые диски, ошибки в программах)
  - Человеческий фактор (забытый ноутбук, потерянная флешка с конфиденциальной информацией, случайное rm -rf * в корне)

И что делать?

Для устранинеия причин нужно разработать политику безопасности (правила, как должно быть) и механизмы защиты (средства, чтобы все было по правилам).

- Аутентификация — кто пытается получить доступ к системе (верен ли введенный пароль)?
- Авторизация — что текущий пользователь может делать (имеет ли прова на запуск программы, на доступ к файлам и т. п.)?
- Контроль — следим, что никто не делает чего-то, что он не должен был делать (поиск и уничтожение вредоносных программ).

Аутентификация

- Пароли
  - Наиболее распространенный механизм
  - Секретный код известный только ползователю и серверу
  - Пользователь, который ввел пароль, получает права того, с кем этот пароль был ассоциирован
- Смарт-карты
  - Физическое устройство, для получения доступа нужно физически украсть карточку
  - На карте есть процессор и память, она может осуществлять шифрование и хранить ключи
  - Защищена внешним паролем (pin-кодом, например)
- Биометрические данные
  - Отпечатки пальцев, тембр голоса, сканирование сетчатки (анализ ДНК?).
  - Довольная высокая степень защиты.
  - Нельзя «поменять пароль».
  - Нельзя одному и тому же пользователю выдать разные права доступа (root и обычный пользователь).

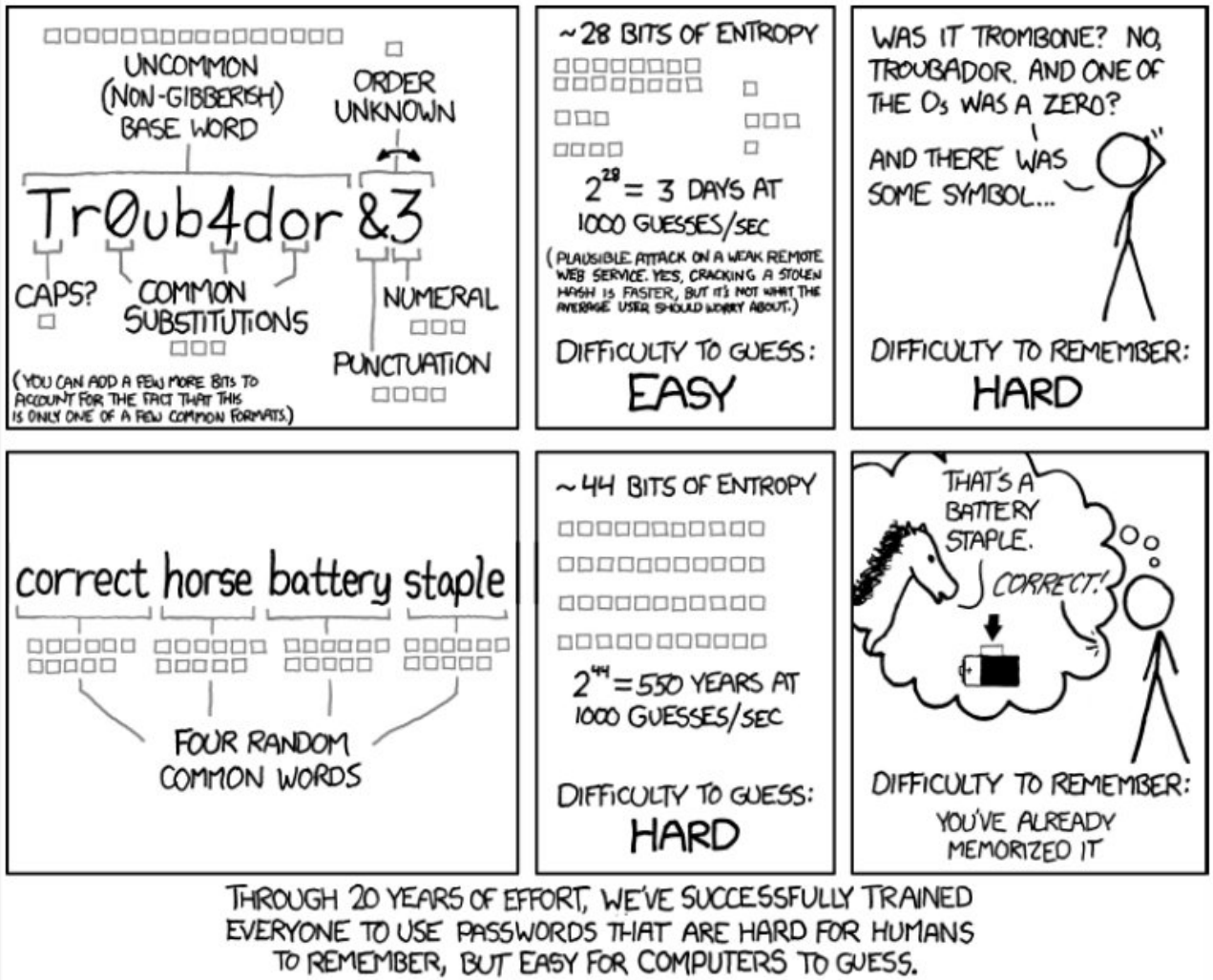
Пароли

- Имя и пароль запрашиваются при логине. Как можно облегчить взломщику задачу:
  - Сообщаем, что именно неверно (имя или пароль).
  - Показываем, из скольки символов состоит пароль пользователя.
  - Показываем символы пароля перед тем, как помять их на точки.
- Пары (имя, пароль) должны где-то храниться в систме (например, в /etc/passwd):
  - Файл паролей может быть открыт на чтение (чтобы получить список пользователей и т. п.)
  - Нужно хранить зашифрованные пароли.

Взлом системы, защищенной паролем

- Угадывание пароля. Зная пользователя и его логин можно попытаться подобрать пароль (дата рождения, имя собаки, город проживания).
- Подбор по словарю. Моррис, Томпсон, 1979 год: 86 % паролей можно подобрать по заранее подготовленному словарю.
- Пароль сложный, его нельзя угадать, но нельзя и запомнить: бумажка на мониторе.
- Подслушивание при логине по сети: telnet, rsh, rlogin без шифрования передавали пароли открытым текстом.

Надежные пароли



Совершенствование безопасности паролей

- Надежные алгоритмы шифрования, запрещение чтения файла с зашифрованными паролями.
- Пароль содержит минимум n символов.
- Пароль обязан содержать буквы разного регистра, цифры и спецсимволы.
- Периодическая смена пароля (одноразовые пароли).

Аутентификация в распределенных системах

Проблема: нужно пересылать пароль по сети.

Требования:

- Только получатель может прочитать, что послал отправитель A.
- Получатель должен быть уверен, что сообщения шлет именно отправитель A.

Средства:

- Шифрование с секретным ключом (симметричное шифрование).
- Шифрование с открытым ключом.

Свойства алгоритмов шифрования

- Алгоритмы шифрования должны быть открыты.
- По зашифрованному тексту невозможно восстановить исходный, не зная ключа.
- По исходному и зашифрованному тексту невозможно восстановить ключ.

Распространение ключей

- При симметричном шифровании:
  - Физически передать ключ (на флешке, в блокноте)
  - Использовать централизованный сервер (например, kerberos).
- При шифровании с открытым ключом:
  - Используется пара ключей: открытый и закрытый. Алгоритмы RSA, DSA.
  - При шифровании: шифруем открытым ключом, только пользователь с закрытым ключом может расшифровать
  - Можно использовать для подписей. Подпись — хеш (MD5, SHA) от документа, зашифрованный закрытым ключом.
  - Открытые ключи должна подписывать авторизованная сторона. Ключи авторизованной стороны известны пользователю (зашиты в браузер, например).

Атаки изнутри системы

- Троянские кони: замаскированные программы, которые помимо своих основных функций выполняют что-то еще. Выполяются с полномочиями запустившего пользователя.
- Логически бомбы. Нечто, заложенное в систему программистом, срабатывающее по его желанию.
- Использоание переполнения буфера (особенно неприятно в программах с SETUID-битом).

Известные проблемы:

- UNIX:
  - lpr позволяла удалить файл после печати: печатаем файл паролей.
  - Связь core файла в домашнем каталоге с /etc/passwd, падение программы с SETUID-битом — запись нужных данных в файл паролей.
  - Червь Морриса: rsh (с одной машины на другую мог быть беспарольный доступ), переполение буфера в программе finger,

Вирусы и антивирусы

Under construction

Проектирование систем безопасности

- Устройство системы не должно быть секретом
- По умолчанию доступ не предоставляется
- Периодическая проверка прав доступа (смена паролей, timespamp в ключах, проверка прав на файлы)
- У каждого проыцесса и пользователя должен быть необходимый минимум привилегий
- Психологически приемлимая система контроля (слишком сложные пароли пишут на листках)
- Сохранение простоты: чем сложнее система, тем больше в ней ошибок.