МЕТОДЫ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы. К сервисам безопасности относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование

Многие механизмы защиты могут быть реализованы как на программном, так и на аппаратном уровне, однако более стойкими считаются аппаратные реализации. Это связано со следующими причинами:

1. Целостность программной защиты легко нарушить, это дает возможность злоумышленнику изменить алгоритм функционирования защиты необходимым образом, например, заставить процедуру контроля электронно-цифровой подписи всегда выдавать верные результаты. Нарушить целостность аппаратных реализаций зачастую невозможно в принципе в силу технологии их производства.

2. Стоимость аппаратных средств защиты во многом повышается благодаря сокрытию защитных механизмов на аппаратном уровне, злоумышленник при этом не может их исследовать в отличие от программной защиты.

Программно-аппаратные средства идентификации и аутентификации пользователей

ПАРОЛЬНЫЕ ПОДСИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Реализуются в открытых компьютерных системах. Являются наиболее распространенными. В качестве идентификации используется имя пользователя, в качестве аутентификации – секретный пароль.

Преимущества: дешевизна, возможность использовать во всех компьютерных системах.

Недостаток: самые уязвимые ко взлому:
- перебор пароля в интерактивном режиме;
- подсмотр, кража из общедоступного места;
- возможность преднамеренной передачи пароля другому лицу;
- кража БД учетных записей из общедоступного места;
- перехват вводимого пароля путем внедрения в КС программных закладок;
- перехват паролей передаваемых по сети;

Для уменьшения влияния человеческого фактора требуется реализовать ряд требований к подсистеме парольной аутентификации

Требования:

1. Задавание минимальной длины пароля для затруднения перебора паролей в лоб;
2. Использование для составления пароля различных групп символов для усложнения перебора;
3. Проверка и отбраковка паролей по словарю;
4. Установка максимальных и минимальных сроков действия паролей;
5. Применения эвристических алгоритмов, бракующих нехорошие пароли;
6. Определение попыток ввода паролей;
7. Использование задержек при вводе неправильных паролей;
8. Поддержка режима принудительной смены пароля;
9. Запрет на выбор паролей самим пользователем и назначение паролей администратором, формирование паролей с помощью автоматических генераторов стойких паролей.

Количественная оценка стойкости парольной защиты

A – мощность алфавита символов, из которых состоит пароль;

L – длина пароля;

V – скорость перебора паролей злоумышленником;

T – срок действия паролей;

P – вероятность подбора паролей злоумышленником за время t, меньшее срока действия паролей

$$P = \frac{V * T}{A^L}$$

Аппаратная защита от несанкционированного доступа

Под инженерно-технической защитой информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

1. Защиту территории и помещений компьютерной системы от проникновения нарушителей;
2. Защиту аппаратных средств компьютерной системы и носителей информации от хищения;
3. Предотвращение возможности удаленного видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств компьютерной системы;
4. Организацию доступа в помещения компьютерной системы сотрудников;

контроль над режимом работы персонала компьютерной системы;

К аппаратным средствам защиты информации относятся:
1. электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие некоторые функции обеспечения информационной безопасности.

К основным аппаратным средствам защиты информации относятся:
2. устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.П.);
3. Устройства для шифрования информации;
4. устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

устройства уничтожения информации на магнитных носителях;

устройства сигнализации о попытках несанкционированных действий пользователей компьютерной системы и др.

СПАСИБО ЗА ВНИМАНИЕ