

Задание

1. Изучить и законспектировать материал лекции.
2. Фотоотчет присылать на электронную почту в трехдневный срок
С уважением, Хвастова Светлана Ивановна
!!! Если возникнут вопросы обращаться по телефону 0721389311
(ватсап). Электронная почта: xvsviv@rambler.ru

Идентификация и аутентификация пользователя. Пароли. Управление привилегиями пользователей базы данных. Безопасность на основе ролей.

Цели изучения темы

- изучить содержание и механизмы реализации сервисов безопасности "идентификация" и "аутентификация".

Требования к знаниям и умениям

Студент должен знать:

- механизмы идентификации и аутентификации;
- идентификаторы, используемые при реализации механизма идентификации и аутентификации.

Студент должен уметь:

- использовать механизмы идентификации и аутентификации для защиты информационных систем.

Ключевой термин

Ключевой термин: идентификация и аутентификации.

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Второстепенные термины

- механизм идентификации;
- механизм аутентификации.

Структурная схема терминов



1. Определение понятий "идентификация" и "аутентификация"

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация

заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

- набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);

- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на **паролях** – конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные (многократно используемые) пароли;

- методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания

пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обуславливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный

защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

2. Механизм идентификация и аутентификация пользователей

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1. Статическая аутентификация.
2. Устойчивая аутентификация.
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

Выводы по теме

1. Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

2. Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

3. **Идентификация** – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

4. **Аутентификация** (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

5. В качестве идентификаторов в системах аутентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи). В системах идентификации такими идентификаторами являются физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

6. В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

7. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия

(совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

8. В целом аутентификация по уровню информационной безопасности делится на три категории: статическая аутентификация, устойчивая аутентификация и постоянная аутентификация.

9. Постоянная аутентификация является наиболее надежной, поскольку обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки.

Контрольные вопросы

1. Что понимается под идентификацией пользователя?
2. Что понимается под аутентификацией пользователей?
3. Применим ли механизм идентификации к процессам? Почему?
4. Перечислите возможные идентификаторы при реализации механизма идентификации.
5. Перечислите возможные идентификаторы при реализации механизма аутентификации.
6. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
7. В чем особенности динамической аутентификации?
8. Опишите механизм аутентификации пользователя.
9. Что такое "электронный ключ"?
10. Перечислите виды аутентификации по уровню информационной безопасности.
11. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?