РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Схема аутентификации пользователей с помощью логинов и паролей.

Казначеев Сергей Ильич

Содержание

Оглавление

1 Введение

Аутентификация пользователей представляет собой фундаментальный механизм информационной безопасности, формирующий первый и важнейший рубеж защиты компьютерных систем. В контексте отечественных операционных систем эволюция механизмов аутентификации отражает не только технологический прогресс, но и ответ на вызовы времени - от обеспечения базовой защиты в ранних ЭВМ до создания сложных многофакторных систем в современных защищённых дистрибутивах.

2 Историческое развитие систем аутентификации

1. Ранние советские ОС (1960-1970-е годы)

Первые механизмы аутентификации в отечественных операционных системах появились вместе с разработкой многопользовательских ОС для БЭСМ-6. Системы “Диспетчер-68” и ОС ИМП использовали элементарные парольные схемы с хранением учетных данных в специальных защищенных областях памяти. Аутентификация проводилась преимущественно на уровне управления вычислительными задачами, что соответствовало архитектурным особенностям этих ранних ЭВМ.

2. ОС для мини-ЭВМ (1970-1980-е годы)

С появлением мини-ЭВМ системы аутентификации претерпели значительные изменения. Операционные системы типа РТ-11 и ДИАЛ перешли к файловому хранению учетных записей, что позволило более гибко управлять правами пользователей. В этот период появились первые реализации базового шифрования паролей и системы разграничения доступа к периферийным устройствам, что было особенно важно для промышленных применений.

3. UNIX-подобные системы (1980-1990-е годы)

Знаковым этапом стало появление UNIX-подобных систем. ОС ДЕМОС, разработанная на базе BSD UNIX, адаптировала классическую UNIX-модель аутентификации с файлом /etc/passwd к отечественным реалиям. Особое внимание было

уделено поддержке кириллицы в учетных записях и разработке механизмов блокировки при многократных неудачных попытках входа - прообраз современных систем защиты от brute-force атак.

3 Современные реализации

1. Безопасное хранение учетных данных

Современные российские ОС используют ГОСТ Р 34.11-2012 “Стрибог” для хэширования паролей. Принцип раздельного хранения, когда хэши паролей вынесены в отдельный файл /etc/shadow с ограниченными правами доступа, стал обязательным требованием. Дополнительно применяются политики сложности паролей, включающие требования к минимальной длине и регулярной смене.

2. Гибкая архитектура аутентификации

Процесс проверки подлинности строится по модульному принципу с использованием Pluggable Authentication Modules (PAM). Это позволяет интегрировать различные методы аутентификации, подключаться к внешним каталогам пользователей и реализовывать многофакторную аутентификацию.

3. Дополнительные защитные механизмы

Современные реализации включают: - Интеграцию с аппаратными токенами - Поддержку двухфакторной аутентификации - Детальное журналирование попыток входа - Механизмы временной блокировки учетных записей

4 Проблемы и перспективы развития

Основные угрозы включают методы перебора паролей и фишинговые атаки. Перспективные направления развития сосредоточены на:

1. Внедрении биометрических методов
2. Использовании криптографических процессоров
3. Развитии непрерывной аутентификации
4. Создании единых центров управления учетными записями

5 Заключение

Эволюция систем аутентификации в отечественных ОС демонстрирует способность российских разработчиков создавать надежные решения, соответствующие международным стандартам и особым требованиям национальной безопасности. Будущее развитие видится в создании адаптивных, “невидимых” для пользователя систем аутентификации.

Список литературы

1. Механизмы аутентификации в отечественных ОС - https://www.computer-museum.ru/histsoft/auth_os.htm
2. История систем защиты информации в СССР - https://ru.wikipedia.org/wiki/История_защиты_информации_в_СССР
3. Аутентификация в ОС ДЕМОС - https://ru.wikipedia.org/wiki/ДЕМОС#Аутентификация
4. Системы защиты в Astra Linux - https://www.astralinux.ru/security/
5. Механизмы PAM в ALT Linux - https://www.altlinux.org/PAM
6. ГОСТ Р 34.11-2012 “Функция хэширования” - https://docs.cntd.ru/document/1200095548