УДК 371.64/.69

ВИКОРИСТАННЯ GSM АВТОРИЗАЦІЇ У СИСТЕМІ ДИСТАНЦІЙНОГО НАВЧАННЯ

Бичков О.С., Смєлов В.В.
Київський національний університет імені Тараса Шевченка

У даній статті розглянута структура програми розширеної авторизації — авторизації зі зворотнім зв'язком. У якості зворотнього зв'язку — користувачу пропонується ввести текст SMS повідомлення, яке йому надсилає програма. У роботі наведені основні етапи взаємодії з GSM терміналом.

Ключові слова: *авторизація; авторизація зі зворотнім зв'язком, розширена авторизація, структура авторизації з використанням GSM термінала.*

Вступ

На сьогоднішній день дистанційна форма навчання стає все більш популярною [1,2]. Але для її функціонування необхідна надійна система аутентифікації користувачів.

Останнім часом все частіше застосовується, так звана, розширена або багатофакторна аутентифікація. Вона побудована на використанні кількох компонент, таких як: інформація, яку користувач знає (пароль), використанні фізичних компонентів (наприклад, смарт-карти), технології ідентифікації особи (біометричні дані), технології, які відрізняють комп'ютерних ботів від користувачів та Feedback авторизації (авторизації зі зворотнім зв’язком).

Актуальність

З розвитком технології з'являється все більше можливостей віддаленого керування об'єктами, але при цьому розвиваються і технології, які можуть перешкоджати коректному керуванню, або ставлять собі за мету перехоплення та змінення команд, що віддаються. Тому безпека є важливою складовою системи дистанційного навчання. Використовуючи мобільні телефони можливо значно збільшити рівень надійності.

При цьому існує декілька способів.

- Користувач отримує і вводить текст SMS повідомлення – такий спосіб буде розглянутий надалі.
- Користувач використовує унікальну програму встановлену на мобільний телефон, яка за введеним текстом генерує вихідний.

Структури, які використовують такого роду системи вважають за потрібніше не афішувати принципи та технічні подробиці функціонування системи з міркувань безпеки.

Слід зазначити, що такі системи контролю чудово підходять для вирішення поставленої проблеми, оскільки вони гарантують надійність та не потребують значних зусиль від користувача.

Мета

У статті ставиться задача створити систему перевірки автентичності особи за допомогою авторизації зі зворотнім зв’язком.

Елементом зворотнього зв’язку буде SMS повідомлення, яке надсилатиметься системою перевірки користувачу за допомогою GSM терміналу.

Доступ до інформації буде надаватися при проходженні як звичайної авторизації (перевірки логіна та пароля) так і авторизації зі зворотнім зв’язком. Доступ до різних частин інформації буде здійснювати лише за умови повторного проходження авторизації зі зворотнім зв’язком. Стандартну авторизацію варто буде проходити лише один раз за сеанс, при першому доступі до матеріалів.

Будемо вважати, що усі потенційні користувачі системи користуються послугами українських телефонних GSM операторів зв’язку, та мають змогу отримувати SMS повідомлення.

Основний результат

Складовими частинами авторизації зі зворотнім зв'язком є:

1. Клієнтська частина.
2. Серверна частина.
3. Робота з GSM терміналом.

Опишемо детальніше особливості роботи кожної з них:

На стороні клієнта буде збиратися інформація про користувача та здійснюватися надсилання її на сервер. Також буде здійснюватися зображення інформації, що буде передаватися з сервера.

Таким чином будуть реалізовані такі механізми:

1. Реєстрації нових користувачів

При реєстрації нового користувача він має надати програмі таку інформацію: свій логін та пароль (для стандартної авторизації), номер свого мобільного телефону (на який будуть надходити SMS повідомлення), додаткову інформацію (якщо така інформація необхідна для інших частин системи дистанційного навчання).

2. Авторизація

При авторизації користувач має ввести логін та пароль, який він вказував при реєстрації.

3. Перевірки SMS повідомлень

Користувачу слід ввести текст SMS повідомлення, яке він отримав.

4. Зображення інформації

Користувачу буде надана змога проглядати інформацію, яка його зацікавила.

У випадку некоректного завершення якоїсь з операцій користувач буде поінформований про характер помилки, та можливі способи вирішення.

Серверна частина буде складатися з двох частин:

1. Обробка даних.
2. Виконання запитів у базі даних.

Бази даних будуть представленні двома таблицями – одна для зберігання інформації про користувачів, інша для зберігання інформації, яка потім зображується.

Механізм SMS авторизації полягає у додатковій перевірці за допомогою SMS повідомлень.

Опишемо детальніше етапи SMS авторизації:

1. Користувач входить в систему – як результат система ідентифікує користувача і "узнає" телефонний номер користувача.
2. Користувач намагається отримати доступ до інформації, яка захищена механізмом SMS авторизації.
3. Система надсилає SMS повідомлення на телефонний номер користувача та зображає поле для вводу тексту повідомлення.
4. Користувач отримує SMS повідомлення та вводить його в необхідне поле.
5. Система перевіряє введений текст і надає, або не надає доступ в залежності від результатів перевірки.

Перехоплення SMS повідомлень є майже неможливим через значний захист цієї технології мобільними операторами.

Розглянемо детальніше реалізацію запропонованого підходу.

Сценарій виконання програми на стороні клієнта матиме такий вигляд:

- Користувач заходить на сторінку, йому пропонується ввести свої дані або зареєструватися.
- Користувач вводить свої дані та відправляє їх на сервер (користувач реєструється).
- У випадку успішного проходження переднього етапу користувач ознайомлюється з наявними розділами.
- Користувач обирає необхідний йому розділ.
- Користувача пропонується ввести SMS повідомлення, яке він отримав.

– Якщо користувач отримав SMS повідомлення та вірно ввів його текст, то він має змогу ознайомитися з інформацією.
– По закінченню перегляду розділу користувач або залишає систему, або переходить по 4 пункту.

Загалом схема роботи сервера матиме такий вигляд (рис.1):

Рис. 1. Схема роботи сервера.

Розглянемо детальніше етапи роботи сервера:

1. Отримання даних від клієнта – це можуть бути логін та пароль, або дані з реєстраційної форми тощо.
2. Відповідно до потрібної функціональності здійснюється перевірка отриманих даних та формування запитів для бази даних.
3. Виконання запитів.
4. В залежності від необхідності відправлення запитів на GSM термінал.
5. Опрацювання помилок, якщо вони виникли та аналіз результатів.
6. Відправлення результатів користувачу.

На будь якому етапі серверна частина виконання може бути перервана, тоді на сторону клієнта передається код помилки, та стек операцій, які до цього призвели. На стороні клієнта ця інформація аналізуються та зображується текстове повідомлення з інформацією про помилку на шляхи її вирішення.

Наведемо схему роботи системи (рис.2).

Рис.2. *Схема роботи системи.*

Уся інформація, окрім лише тієї, яку треба зобразити як шукану, передається лише на сервер. Сервер в свою чергу лише говорить чи успішною були авторизація, чи правильно введений текст SMS повідомлення тощо. Тобто перехопити правильні SMS повідомлення неможливо, оскільки їх текст курсує лише від клієнта до сервера, і не навпаки.

Текст SMS повідомлення формується на стороні сервера та заноситься в базу даних, при перевірці введений текст порівнюється з тим що знаходиться в базі даних. Інформація, яка приходить з сервера на сторону клієнта проходить процедуру серіалізації.

Висновки.

Авторами були розглянуті та впроваджені основні концепції авторизації зі зворотнім зв'язком з використанням GSM термінала. Були наведені структурні схеми та пояснення до усіх етапів функціонування системи. Запропонована концепція авторизації може бути застосована у багатьох сферах, оскільки є досить гнучкою та надзвичайно надійною.

Подальший розвиток можна спрямувати на шифрування інформації, яка передається з сервера на сторону клієнта з метою підвищення рівня безпеки. Зараз авторами розробляється комплекс програм, які б унеможливлювали несанкціоноване копіювання зображуваної інформації з навчального сервера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Співаковський О.В., Львов М.С., Кравцов Г.М., Федорова Я.Б., Осипова Н.В., Кушнір Н.О. Цілі та задачі проекту «Створення банку електронних документів з дистанційного навчання для вищої педагогічної освіти» // Інформаційні технології в освіті. – в.4. – 2009. – С.96-110.
2. Бичков О.С.. Черний Ю.В. Використання сучасних інформаційних технологій у навчальному процесі // Вісник Київського національного університету імені Тараса Шевченка. Філософія. Політологія. Вип.94-96. – 2010. – С.17-20.