НАПРЯМ 5. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

DOI https://doi.org/10.36059/978-966-397-357-9-112

ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Аністратенко М. В.
магістр за спеціальністю 125 – Кібербезпека
Міжнародний гуманітарний університет
м. Одеса, Україна

Перуцький О. В.
магістр за спеціальністю 125 – Кібербезпека
Міжнародний гуманітарний університет
Науковий керівник: ***Йона Л. Г.***
кандидат технічних наук, доцент
Міжнародний гуманітарний університет
м. Одеса, Україна

З розвиненням інформаційних технологій майже у всіх сферах життя людини, виникає проблема із захистом інформаційних систем. Технічний прогрес в інформаційних технологіях стрімко розвивається, тому і зловмисники, які хочуть заволодіти інформацією, постійно удосконалюють свої знання та вигадують нові способи заволодіння даними.

Під час обробки інформації з обмеженим доступом необхідно забезпечувати її захист від несанкціонованого перегляду, змін, видалення, копіювання, поширення.

Перевірка авторського права та справжності користувача, захист конфіденційності, цілісності та доступності інформації, реалізується за допомогою програмних, програмно-апаратних та апаратних засобів шляхом криптографічного перетворення даних з використанням ключової інформації.

Існують різні алгоритми криптографічного перетворення інформації. Криптографічні алгоритми можна поділити на 2 класи: симетричні та асиметричні. Алгоритми, які об’єднують обидва класи називаються гібридними.

Симетричні алгоритми характеризуються тим, що зашифрування та розшифровування відбувається за допомогою одного спільного секретного ключа шифрування.

Асиметричні алгоритми характеризуються тим, що вони крім секретного ключа мають відкритий (публічний ключ).

Частіше асиметричні системи використовуються для автентифікації документів та розподілу ключів.

Наявність процедур ідентифікації та автентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з поіменованими суб'єктами і об'єктами інформаційних систем.

Для правильного тлумачення, необхідно розрізняти такі основні поняття, як ідентифікація, автентифікація та авторизація.

Ідентифікація – це процес розпізнавання користувача.

Автентифікація – це підтвердження автентичності, тобто проходження перевірки справжності користувача. Ця процедура відбувається на вході в систему, перед тим, як користувач увійде до неї.

Авторизація – це надання повноважень користувачеві і перевірка прав на вчинення якихось дій у системі. Ця процедура відбувається після входу до системи.

При проходженні процедури автентифікації, інформаційна система перевіряє відповідність наданих користувачем даних з тим, що зберігається в її базі даних. По-перше, система має з'ясувати чи існує користувач з таким ім'ям. По-друге, перевіряється збіг введеного користувачем паролю з його обліковим записом. Далі система може затребувати сертифікат, IP-адресу чи додатковий код верифікації. Після отримання правильних відповідей, користувачеві надається допуск до системи.

Методи автентифікації можуть бути однофакторними, двофакторними, три– …, тобто багатофакторними. Отже, якщо підтвердження справжності відбувається за якимось одним фактором, то це буде однофакторна автентифікація. Якщо для автентифікації користувача використовується кілька факторів, то це вже може бути багатофакторна автентифікація.

Щодо факторів, за якими відбувається перевірка справжності користувача, то вони поділяються за трьома напрямами: *знань* (те, ЩО людині відомо, наприклад, відповідь на якесь таємне запитання); *володіння* (те, ЧИМ людина володіє та може це продемонструвати, наприклад, якийсь фізичний об'єкт, телефон, платіжна картка, флешка, тощо); *властивості* (деякі фізичні властивості, наприклад, біометрична характеристика, жест або модель поведінки). У таблиці 1 показано класифікацію факторів автентифікації з прикладами.

Таблиця 1

Класифікація факторів автентифікації

ФАКТОР АВТЕНТИФІКАЦІЇ					
ЗНАННЯ	**ВОЛОДІННЯ**	**ВЛАСТИВОСТІ**			
		Біометричні		**За дією**	**За місцем**
		Статичні	***Динамічні***		
PIN	Ключ	Відбиток пальця, губ	Голос	Жест	Розташування
Кодова фраза	USB– токен	Сітківка, райдужна оболонка ока	Динаміка підпису	Підпис	Позиція на поточний час
Пароль	Смартфон	Геометрія обличчя, долоні	Клавіатурний почерк	Електронний підпис	
	Картка	ДНК	Рух губ		
		Форма черепа, вуха	Хода		
		Зображення вен	Почерк		

Для підвищення точності системи автентифікації зазвичай використовують багатофакторну автентифікацію. Наприклад, для перевірки справжності користувача система може запросити введення паролю та якийсь біометричний параметр людини. При цьому, для підвищення точності біометричної системи враховується значення *коефіцієнту помилкового збігу* (ймовірність того, що системою невірно відбудеться порівняння вхідного зразка з еталоном, який є у базі даних) та *коефіцієнту помилкової розбіжності* (ймовірність того, що системою помилково не буде розпізнаний справжній вхідний зразок користувача). Ці коефіцієнти ще можна знайти в літературі під назвою помилка I типу та помилка II типу відповідно, та відображають спроможність системи обмежувати вхід авторизованим користувачам. Системи з низькою пороговою величиною коефіцієнту помилкового збігу більш захищені, проте системи з низьким порогом коефіцієнту помилкової розбіжності є більш зручними у використанні. Тому при налаштуванні системи автентифікації, необхідно знайти компроміс між безпекою та простотою використання.

Можна проаналізувати методи автентифікації, що найчастіше застосовуються користувачами за такими критеріями, як: зручність, безпека, вартість, актуальність чи можливість використання в наявній інфраструктурі. У таблиці 2 показано частоту використання методів автентифікації за певними критеріями.

Таблиця 2

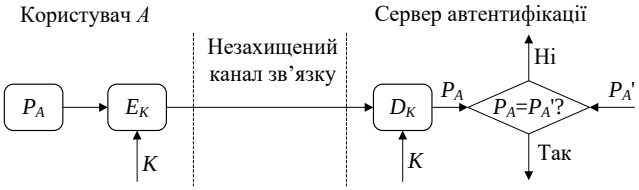
Частота використання методів автентифікації у системах захисту

Критерії Захисту	**Методи автентифікації**							
	PIN	Пароль	Картка	Відбиток пальця	Підпис	Сітківка ока	ДНК	ЕП
Безпека	**	**	**	**	**	***	***	***
Зручність	***	***	***	***	**	**	*	**
Актуальність	***	***	***	**	**	**	*	**
Вартість	***	***	***	**	**	**	*	*

** – мало; ** – часто; *** – дуже часто*

В процесі пересилання даних для проведення процесу автентифікації, ці дані необхідно шифрувати. Це є необхідною умовою роботи системи для того, щоби зловмисник не зміг скористатися перехопленим повідомленням.

На Рис.1 показано схему простої автентифікації користувача, де видно, що перед пересиланням пароля P_A, що надав користувач, відбувається його шифрування секретним ключем K. На приймальній стороні цей пароль відновлюється шляхом розшифровування секретним ключем та порівнюється з еталоном паролю, що зберігається в базі даних системи [1].



P_A – пароль користувача A ; K – ключ шифрування;
E_K – функція зашифрування; D_K – функція розшифрування.

Рис. 1. Схема простої автентифікації користувача

Для процесу автентифікації існує також схема простої автентифікації з використанням односторонньої функції для перевірки пароля. В цьому разі підвищується рівень безпеки процесу автентифікації, тому що перевірка відбувається після застосування односторонньої функції до паролю. Результат перетворення порівнюється зі значенням, що зберігається в ідентифікаційній таблиці паролів для даного користувача. У такій схемі простої автентифікації передача ідентифікатора користувача та відповідного пароля може здійснюватися у такий спосіб:

а) в захищеному вигляді, коли всі дані зашифровані;

б) паролі передаються у незахищеній формі, приміром за протоколом парольної автентифікації PAP (Password Authentication Protocol).

Очікувано, що системи автентифікації, які побудовані на символьних паролях, з міркувань безпечності, будуть замінені на системи, засновані на графічних паролях. Проте, незручності, що виникають при введенні графічного пароля обмежують його використання в простих системах автентифікації.

Можна зробити висновки, що перспективним напрямком розвитку є системи багатофакторної автентифікації, де в якості основного фактору буде застосовуватись біометрична характеристика людини. Основні зусилля в цьому напрямку спрямовані на вдосконалення апаратного та програмного забезпечення для зниження рівня помилок I типу та II типу.

Література:

1. Системи банківської безпеки / Л.Г. Йона, О.В. Онацький, О.В. Швець // Навчальний посібник. 2021, 58 с.

DOI https://doi.org/10.36059/978-966-397-357-9-113

МЕТОД ПОШУКУ ПАТОЛОГІЙ СЕРЦЯ ЗА ЗОБРАЖЕННЯМ ЕЛЕКТРОКАРДІОГРАМИ З ВИКОРИСТАННЯМ ANDROID STUDIO

Атаулін О. А.
здобувач вищої освіти другого (магістерського) рівня
за спеціальністю 122 – Комп'ютерні науки
Міжнародний гуманітарний університет
м. Одеса, Україна

Биков Р. Г.
викладач кафедри інформаційних технологій
Міжнародний гуманітарний університет
м. Одеса, Україна

У наш час питання спостереження за здоров'ям є дуже актуальним, особливо у зв'язку з поширеністю серцево-судинних захворювань. Серцево-судинні захворювання залишаються на першій позиції серед причин смертності, що підкреслює важливість своєчасного визначення цих захворювань та необхідність розвитку технологій для їх