4. К. Ша, У. Вей, Т. Ендрю Янг, З. Ванг, У. Ши. Про проблеми безпеки та відкриті проблеми в Інтернеті речей // Наступ. Генер. Обчислення. Сист. – 2018 – №83.

5. М. Чернишев, З. Байг, О. Белло, С. Зеадалі. Інтернет речей (IoT): Дослідження // IEEE Інтернет речей, журнал – 2018 – №5. 1637–1647.

6. С. Сінгх. Розширені легкі алгоритми шифрування пристроїв IoT: опитування, виклики та рішення // Інтел. Гуманіз. Обчислення – 2017.

7. Х.З. Ячень Ян, Лонгфей Ву, Гуйчен Інь, Ліє Лі. Огляд з питань безпеки та конфіденційності в Інтернеті речей // Інт. Конф. Інтернет Технол. Зах. – 2015. – 202–207 с.

УДК 004.056.53

КЛАСИФІКАЦІЯ ВИДІВ АВТЕНТИФІКАЦІЇ

К.О. Діденко, Ю.А. Мілінчук
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Атаки на системи автентифікації, на жаль, не рідкісне явище в наш час і багато статей присвячені різноманітним методам, видам та способам автентифікації. Для легшого розуміння кожного з видів, потрібно знати, які методи та способи можна використовувати і які типи протоколів при цьому застосовуються.

Саме автентифікація являє собою процедуру перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту. [1] Ця процедура може виконуватись за допомогою наступних методів:

- парольні, в яких може використовуватись одноразові або багаторазові паролі;
- Public Key Infrastructure (PKI), заснований на асиметричній криптографії, де закритий ключ користувача може бути на смарт карті, криптографічному токені або знімному накопичувачі;
- мобільна автентифікація, де, за допомогою спеціальної програми, на смартфоні генерується одноразовий пароль (one time password, OTP). Таким чином, смартфон виступає OTP токеном; [2]
- біометричні, де перевірка проходить за фізіологічними характеристиками користувача;
- інформація користувача, до якої відноситься номер телефону, дівоче прізвище матері, дата реєстрації та інше, що може використовуватись для відновлення логіна і пароля або для двофакторної автентифікації;
- користувацькі дані, де використовуються інформація про точки доступу бездротового зв'язку та геодані про місце знаходження користувача. [3]

Способи можна класифікувати наступним чином [4]:

- базова автентифікація, при застосуванні якої логін і пароль користувача входять до складу веб-запиту. Будь-який зловмисник, що перехоплює пакети інформації легко впізнає засекречені дані;

– дайджест-автентифікація. Вид автентифікації, який має на увазі передачу призначених для користувача паролів в хешованому стані. Постійне оновлення хешу не дає зловмиснику можливості розшифрувати пакет даних - кожне нове підключення утворює інше значення пароля;

– HTTPS дає можливість шифрування не тільки логіна і пароля користувача, але і всіх інших даних, що передаються між інтернет-клієнтом і сервером;

– автентифікація з пред'явленням цифрового сертифікату, що має на увазі використання протоколів із запитом і відповіддю на нього;

– автентифікація з використанням Cookies. Браузер, при кожній спробі підключення до ресурсу, посилає Cookies як одну із складових частин HTTP-запиту;

– децентралізована автентифікація, за принципом якої працюють такі протоколи, як OpenID, OpenAuth та OAuth.

В залежності від кількості методів, що використовуються, автентифікація поділяється на однофакторну та багатофакторну, де використовується декілька методів.

Залежно від можливостей засобів автентифікації і рівня інформаційної безпеки, можна виділити наступні види автентифікації:

– статична автентифікація. Захищає від несанкціонованого доступу зловмисників, які можуть заволодіти даними про ідентифікатор користувача під час його роботи з інформаційним ресурсом або сайтом. Найпоширенішим методом, що забезпечує даний вид, є використання багаторазових паролів;

– стійка, механізм якої заснований на використанні динамічних ідентифікаторів, які змінюються перед кожним сеансом. Даний вид не захищає від активний атак;

– постійна, що захищає суб'єкта від несанкціонованої крадіжки і модифікації його ідентифікатора на будь-якому етапі роботи з інформацією. Цей вид забезпечує захист від атак навіть після автентифікації.

В залежності від політики безпеки систем та рівня довіри існує:

– одностороння автентифікація. Користувач доводить право доступу до ресурсу його власнику;

– взаємна. Перевіряється автентичність прав доступу і користувача і власника. Для цього використовують криптографічні способи. [5]

Також, слід розуміти, що автентифікація представляє собою процес порівняння інформації, наданої користувачем, з тією, що знає система. І залежно від типу інформації, її можна віднести до одного з наступних факторів [6]:

– фактор знання – щось, що користувач знає. Це може бути пароль або відповідь на секретне питання;

– речовий фактор – щось, чим користувач володіє. Це можуть бути смарт-картки, токени та інше;

– біофактор – щось, що є частиною користувача. Біометричні сканери розпізнають відбитки пальців, геометрію руки, почерк, голос користувача.

Тож, поєднавши наведену вище інформацію, можна скласти таблицю класифікації видів автентифікації.

Таблиця 1

Класифікація видів автентифікації

Метод	Фактор	Тип інформації	Вид
парольний	знання	багаторазовий пароль	статична
інформація користувача	знання	інформація, що знає тільки користувач	статична
парольний	знання	одноразовий пароль	стійка
мобільна автентифікація	речовий	одноразовий пароль, що генерується на смартфоні, який виступає OTP токеном	стійка
користувацькі дані	знання	геодані, інформація про точки доступу бездротової мережі	стійка
біометричний	біофактор	фізіологічні характеристики	стійка
PKI	речовий	ключ в смарт-карті, токені, знімному накопичувачі	стійка

Потрібно зауважити, що:

– залежно від виду автентифікації, дані методи можна реалізувати різними способами, описаними вище;

– до постійної автентифікації, з найбільш високим рівнем інформаційної безпеки, можна віднести багатофакторну автентифікацію, з використанням декількох методів;

– найбільш оптимальним варіантом можна вважати двофакторну автентифікацію з використанням статичного та стійкого видів, наприклад багаторазового та одноразового паролів, або багаторазового паролю та біометричного методу.

Висновки. Таким чином, запропонована класифікація може допомогти визначити вид автентифікації за методами, факторами та необхідною для автентифікації інформацією, та обрати необхідні методи багатофакторної автентифікації для забезпечення оптимального рівня інформаційної безпеки. Також, дану класифікацію можна використовувати для подальших досліджень, пов’язаних з процедурою автентифікації.

ПЕРЕЛІК ПОСИЛАНЬ:

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу».

2. Методы аутентификации [Електронний ресурс]. – Режим доступу: https://powersecurity.org/ru/blog/authentication-methods/

3. Что такое Аутентификация – Значение [Електронний ресурс]. – Режим доступу: https://sendpulse.ua/support/glossary/authentication

4. Что такое аутентификация [Електронний ресурс]. – Режим доступу: https://www.unisender.com/ru/support/about/glossary/chto-takoe-email-autentifikaciya/

5. Аутентификация [Електронний ресурс]. – Режим доступу: https://promopult.ru/library/Аутентификация

6. Классификация механизмов аутентификации пользователей и их обзор [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/177551/
УДК 004.94

ПРОЕКТУВАННЯ ТА ОПТИМІЗАЦІЯ КОМП'ЮТЕРНОЇ МОДЕЛІ ШТАМПОВИХ ПЛИТ

І.С. Дмитрієва, О.А. Зеленський, Г.Ю. Станчиц
(Україна, Дніпро, Національна металургійна академія України)

Актуальність роботи. В наші дні штампування - це один з прогресивних способів для отримання виробів. Показники економіки операцій штампування визначаються, в більшій мірі, вартістю самого штампового остраху, що припадає на одиницю виробу. У свою чергу вартість самого штампа складається з безлічі факторів: самої конструкції і її технологічності, геометрично-конструктивних параметрів, а також матеріалу, з якого виготовлений, власне, сам штамп. Одним з важливих показників якості штампа є його стійкість, від якої потерпають на кінцевій вартості оснащення, тому, для підвищення рентабельності обладнання, необхідно звернути увагу на цей показник. У процесі підготовки виробництва нових виробів трудомісткість проектування може становити до 50%. Скоротити цей відсоток допомагають САПР. Щоб мінімізувати всі витрати на етапі конструювання вже закладається вибір найбільш раціональної конструкції деталі, зокрема і штампових плит.

Геометрична оптимізація в середовищі чисельного моделювання. Системи автоматизованого проектування (САПР) міцно увійшли в промисловість, так як завдяки їм створення процесів, проектування оснащення помітно прискорюється, дозволяючи спроектувати модель об'єкта і його поведінку в середовищі чисельного моделювання, ще задовго до того, як це буде матеріалізовано.

Алгоритм роботи в системах САПР за умови, що використовується інженерний аналіз починається з параметризації, здійснення якої відбувається в середовищі CAD системи шляхом завдання певних параметрів, що визначають геометрію сплайнів, що надалі сформує геометрію конструкції. Далі проводиться експорт моделі з CAD в CAE, де відбувається етап створення сітки кінцевих елементів для моделі, рішення задач механіки, що включають обчислення цільового функціоналу і обмежень.

Це означає, що будь-яка зміна геометрії моделі CAD системі, спричиняє за собою перерахунок в системі CAE, так як доводиться знову перебудовувати звичайно елементну сітку, складати схему навантажень, задавати обмеження. Так відбувається по циклічній схемі поки конструктор не доб'ється потрібного йому результату. На практиці на створення і перевірку кінцево-елементної сітки йде помітна частина часу, як і на створення схеми навантаження.

Підготовчим етапом перед процесом геометричній оптимізації є робота в середовищі CAD для безпосереднього проектування штампового плити.