УДК 004.056.53- 004.056.52
А.М. Луцків канд. техн. наук, доц., О.І. Крутиголова
Тернопільський національний технічний університет імені Івана Пулюя, Україна

КРИТЕРІЇ ВИБОРУ СИСТЕМ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

A.M. Lutskiv Ph.D. Prof., O.I. Krutyholova
SELECTION CRITERIA OF BIOMETRIC AUTHENTICATION SYSTEMS

Актуальність створення зручних та надійних систем аутентифікації зумовлена зростанням кількості електронних систем із якими взаємодія людина. Такі електронні системи застосовуються практично в усіх сферах життєдіяльності людини: банківському секторі, транспорті (бронювання, замовлення та придбання квитків), освіті (системи дистанційного навчання), медицині (телемедицина), промисловості й виробництві (керування та моніторинг промислових систем), а також у сфері безпеки та оборони країни. У низці випадків питання доступу законного користувача до його даних є доволі критичним, зокрема, це стосується так званих *критично важливих систем*, у яких аутентифікація й всі наступні дії після авторизації мають відслідковуватись та фіксуватись у електронному журналі. Способи доступу користувачів (операторів) у електронні системи є доволі різноманітними й визначаються середовищем у якому працює користувач: персональний комп'ютер, планшет, смартфон, або спеціалізоване автоматизоване робоче місце. Обладнання, за допомогою якого користувач проходить аутентифікацію також може бути доволі різноманітним й залежати від важливості даних та інших технічних особливостей автоматизованих систем. У більшості випадків, показник захищеності комп'ютеризованих систем є величиною обернено пропорційною до зручності (*англ.* usability). Водночас поширеність інформаційних комп'ютеризованих систем у нашому повсякденному житті вказує на те, що фактор зручності є доволі важливим. У ході дослідження аналізується питання зручності систем аутентифікації та критерії їх вибору.

Аутентифікація оператора у комп'ютеризованих системах – перевірка відповідності суб'єкта і того за кого він себе намагається видати, за допомогою деякої унікальної інформації (паролю, відбитку пальця, голосу і т.п.), у найпростішому випадку, за допомогою реєстраційного імені і паролю. Аутентифікацію в інформаційній системі може пройти зареєстрована особа або зловмисник, видавши себе за зареєстровану особу. У результаті успішної аутентифікацію система авторизує користувача. Надійність системи аутентифікації визначається наступними характеристиками:

– FRR (False Rejection Rate) – не допущення законного власника до системи, або помилка першого роду;

– FAR (False Acceptance Rate) – хибний пропуск зловмисника в систему, або помилка другого роду;

– EER (Equal Error Rate) – співвідношення помилок першого та другого роду.

Чим нижчим є параметр EER, тим точнішою буде система біометричної аутентифікації. Водночас, не завжди цей параметр є репрезентативним, й до уваги беруться помилки першого та другого роду. Дуже часто FRR та FAR подаються як оцінки ймовірностей на основі експериментальних даних.

Зручність системи аутентифікації – це міра, відповідно до якої, система аутентифікації може використовуватися особою на максимально комфортному рівні.

Таким чином, система аутентифікації, яка відповідає критерію зручності, гарантує захищеність інформації при найбільш зручних можливостях її використання з належною продуктивністю, ефективністю і задоволеністю. Питання зручності взаємодії користувача з комп'ютеризованими системами висвітлено в міжнародних стандартах ISO/IEC 14754, ISO 13407, ISO 9241-11 та інших [1].

Дослідженням зручності систем аутентифікації займалась велика кількість вчених [2, 3]: Дженіфер Голдбек, Хільмі Гюнес Каячік, Майк Джаст, Лінні Бейлі, Девід Аспінол. До характеристик зручності системи аутентифікації належать:

– швидкість – як швидко може задача може бути виконана користувачем (кількісний показник, вимірюється час);

– ефективність – скільки помилок буде зроблено при виконанні завдання користувачем (кількісний показник, кількість помилок);

– простота навчання – наскільки легким є навчання користування системою (кількісний показник, вимірюється час вивчення);

– легка запам’ятовуваність – здатність легко запам’ятатись користувачем (кількісний показник, вимірюється час аутентифікації при кількох наступних входах і чим він більший, тим гіршою є система).

Після вимірювання параметрів зручності кількох альтернативних варіантів систем аутентифікації можна по кожному із них виставити відносні оцінки й приймати рішення про використання тієї чи іншої системи. Відповідно, критерієм вибору є деякий інтегральний показник, який чітко вказує на вибір тієї чи іншої системи. Водночас, з метою підвищення рівня надійності інформаційної системи від несанкціонованого доступу можна використати багатофакторну аутентифікацію. Один із підходів до вибору методів аутентифікації запропонований у [4].

Іншим важливим, на думку авторів, параметром є критерій доступності за ціною. Цей критерій враховує поширеність та доступність для користувача типових засобів, які можуть їх аутентифікувати: камера, мікрофон, сенсорний екран тощо. Очевидно[4], що аутентифікація за малюнком сітківки ока, теоретично є надійним методом аутентифікації, проте вартість такої системи є достатньо високою. Застосування доступного обладнання, також має іншу перевагу — збільшується коло потенційних користувачів, а відповідно й тестувальників таких систем, що дає змогу краще апробувати такі системи.

Таким чином ключовими критеріями вибору системи аутентифікації є:

– параметри помилок 1-го та 2-го роду;

– інтегральний показник зручності, як сума відносних оцінок;

– фактор ціни та доступності.

Література

1. A European Union project that provides usability and user centred design resources to practitioners, managers and EU projects. [Electronic resource] Access mode: URL: http://www.usabilitynet.org/home.htm

2. Scott Ruoti, Brent Roberts, Kent Seamons Authentication Melee: A Usability Analysis of Seven Web Authentication Systems // Internet Security Research Lab - 2011. P. 916-926.

3. Mike Just, Lynne Baillie, David Aspinall, Edinburgh, U.K.Data Driven Authentication: On the Effectiveness ofUser Behaviour Modelling with Mobile Device Sensors // Appear in MoST 14 workshop - 2013. C. 1-10.

4. Олешко І. В. Моделі та методи оцінки захищеності механізмів багатофакторної автентифікації від несанкціонованого доступу // Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук - 2014. С. 1-26.