чів шифрування. Такими ключами шифрування в запропонованому алгоритмі є початкова умова v_0 та параметр r логістичного відображення. Вибір способу генерації рівня також можна рахувати як ключ, тому що для його генерації можна використати й інші динамічні системи.

Атрактор Лоренца [2] є тримірним представленням «об'єкта», де три просторові координати якого (вісі X, Y та Z) контролюються нелінійними диференційними рівняннями (1):

$$\left\{\begin{array}{l} \dot{x} = -\sigma(x-y), \\ \dot{y} = Rx - y - xz, \\ \dot{z} = bz + xy. \end{array}\right\}, \quad (1)$$

де σ називається числом Прандтля, R називається числом Рейнольдса, причому $\sigma, R, b > 0$, але зазвичай приймають значення $\sigma = 10$, $b = 8/3$, $R = 28$, при яких система володіє хаосом. Кожне рівняння системи Лоренца володіє початковою умовою та параметрами, і демонструє непередбачувану зміну з часом поведінки кожної змінної.

Другою динамічною системою є одномірне логістичне відображення (2):

$$v_{n+1} = r v_n (1 - v_n), \quad (2)$$

де v_n та r – змінна системи та параметр системи відповідно, n – номер ітерацій. Коли $3{,}57 < r < 4$, то починається хаотична поведінка системи [2]. Значення v_n змінюється без періодичності, такий хаос називається детермінованим, оскільки існує чіткий строго визначений закон, за яким можна визначити значення змінної на будь-якій ітерації, починаючи від вибраного початкового значення.

Надійна криптосистема повинна володіти наступними властивостями: чутливістю до вхідного повідомлення (зміна в вхідному повідомленні утворює інший шифр навіть при одному і тому самому згенерованому ключі), чутливістю до початкових умов та параметрів при генерації ключової послідовності, що використовується для шифрування (зміна хоча б одного з параметрів динамічної системи чи початкової умови приводить до генерації іншої ключової послідовності та утворює цілком інший шифр) [3 4]. Оскільки криптосистема має справу з бінарними послідовностями (вхідна інформація та ключова послідовність є наборами логічних 0 та 1), генератор ключа генерує неперервно значення, то формат вихідного зашифрованого повідомлення буде залежати тільки від формату інформації, що ми хочемо зашифрувати.

Властивості динамічних систем дозволяють нам генерувати велику кількість ключів шифрування, і тому забезпечують високу захищеність хаотичної криптосистеми. Це все робить криптосистему стійкою проти різного роду статистичних атак і також роблять атаку грубої сили дуже витратною з точки зору необхідного часу для її реалізації. Навіть якщо зловмисник спробує її провести він потратить на атаку грубої сили дуже багато часу, щоб перебрати всі можливі комбінації ключів, яких для запропонованої точності в 10 знаків після коми, буде велика кількість 10^{50}і на момент розкриття інформації вона може втратити вже свою актуальність.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. *В.С. Анищенко,* Детерминированный хаос, Соросовский образовательный журнал (1997), no. 6, 70-76.
2. *M.S. Baptista,* Cryptography with chaos, Physics Letters A 240 (1998), no. 1–2, 50–54.
3. *P.G. Vaidyaand S. Angadi,* Decoding chaotic cryp-tography without access to the super key. Chaos, Solitons and Fractals, 17: 379-386, 2003.
4. *E.Solak* Cryptanalysis of observer based discrete-time chaot icencryption schemes. International Journal of Bifurcation and Chaos, 15(2): 653-658, 2005.

УДК 681.3

МАЗНИЧЕНКО Н.І., КОШЕВА Н.А.
Національний юридичний університет ім. Ярослава Мудрого (Україна)

СПОСОБИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ

Розглянуті сучасні підходи в задачах ідентифікації користувачів комп'ютерних систем, пе-

реваги та недоліки кожного з них. На основі аналізу зроблені деякі пропозиції, метою яких є підвищення надійності існуючих систем ідентифікації користувачів.

З появою і розвитком нових інформаційних технологій стала актуальна проблема інформаційної безпеки, пов'язана із забезпеченням безпечного збереження і конфіденційності інформації, що оброблюється та зберігається в комп'ютерних системах. Актуальність задачі інформаційної безпеки набуває ще більшої значущості у зв'язку зі зростанням злочинності в сфері використання комп'ютерної інформації. Враховуючи різноманіття потенційних погроз інформації, безпечне збереження і конфіденційність інформації може бути досягнута тільки шляхом створення комплексної системи захисту інформації. Одним з основних і невід'ємних елементів комплексної системи безпеки є підсистема управління доступом до інформаційних ресурсів. Система ідентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу будь-якої інформаційної комп'ютерної системи [1]. Доступ користувачів до різних класів інформації визначається ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача.

Сьогодні існують наступні найпоширеніші підходи до ідентифікації користувачів:

1). Парольна ідентифікація. Суть її зводиться до наступного. Кожен зареєстрований користувач будь-якої комп'ютерної системи одержує набір персональних реквізитів (найчастіше використаються пари логин-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особу та ідентифікує її.

Головна перевага парольної ідентифікації - це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною.

Тепер перейдемо до недоліків. На жаль, їх багато. І самий, мабуть, головний - величезна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

2). Апаратна (електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні [2]. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера.

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, у них реалізовано чимало різних захисних механізмів.

Ну а тепер поговоримо про недоліки апаратної ідентифікації. Мабуть, найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології - ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте, для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися, можуть бути загублені і т.д.

3). Біометрична ідентифікація. Біометрія – це ідентифікація людини по унікальним, властивим тільки йому біологічним ознакам [3]. Тобто, можна сказати, що біометричні технології розроблялися для точного встановлення особи людини, тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак.

Серед біометричних механізмів ідентифікації можна виділити такі:

– по статичних ознаках — те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);

– по динамічних ознаках — поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів ідентифікації користувача на сьогодні використовуються наступні: ідентифікація по відбитку пальця; по розташуванню вен на долоні; по сітківці ока; по веселковій оболонці ока; за формою грона руки; за формою обличчя.

Серед динамічних методів можна назвати наступні: ідентифікація по голосу; по почерку; по клавіатурному почерку.

При всьому теоретичному різноманітті біометричних методів тих, що застосовуються на практиці серед них небагато. Основних методів три - розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по веселковій оболонці або сітківці ока.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до системи, необхідно придбати власний сканер. Але слід відзначити, що останнім часом ціни на біометричні пристрої постійно знижуються.

4). Багатофакторна ідентифікація. В цьому випадку для визначення особи застосовується відразу кілька параметрів [4]. Причому комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні найчастіше використається тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбора його пароля зловмисником (без електронного ключа пароль працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

Впровадження комбінованих систем суттєво збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку.

На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації користувачів інформаційних комп’ютерних систем можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту, парольний захист сам по собі не може забезпечити серйозного захисту. Досить розповсюдженими в якості ідентифікаторів використовуються також різноманітні електронні ключі (токени, карти і т.і.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних комп’ютерних систем.

Таким чином, розглянувши різні технології ідентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде вживання систем багатофакторної ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп’ютерних систем, що дозволяє значно підвищити надійність та точність подібних систем.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004 г. – 384с.
2. Джхунян, В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с.
3. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
4. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. - 2004. - №45.

УДК 517.957

МАМАЙ Л.М.
ДВНЗ “УжНУ” (Україна)

ПРО РЕАЛІЗАЦІЮ ПАРАЛЕЛЬНОГО $\mathcal{AS}$ – АЛГОРИТМА З ВИКОРИСТАННЯМ МОВИ АДА95

Ефективне застосування паралельних обчислювальних систем (ПОС) для розв’язання склад-