УДК 681.3.06

ОСНОВНІ АСПЕКТИ ЗАХИЩЕНОСТІ МЕХАНІЗМІВ АВТЕНТИФІКАЦІЇ PIV-КАРТКИ

Д.С. БАЛАГУРА, Д.В. ІВАНЕНКО

В даній статті викладено результати аналізу загроз механізмів автентифікації, була запропонована модель загроз та вимоги до неї, надані рекомендації щодо перекриття імовірності загроз.

Ключові слова: загроза, автентифікація, модель загроз, біометрика, рекомендації.

Метою цієї роботи є проведення аналізу загроз механізмів автентифікації, побудова моделі загроз та вимоги до неї, надання рекомендацій щодо перекриття імовірних загроз.

ВСТУП

На сучасному етапі у світі набули широкого попиту системи контролю доступу, які дозволяють забезпечити належний рівень автентифікації особи, що сформувала запит до системи, та відповіді на електронний запит. Зважаючи на актуальність зазначених систем, постає задача створення технічних рекомендацій щодо створення таких систем. Першою країною, яка вирішила це питання, стали США, які затвердили стандарт – FIPS 201 Personal Identity Verification of Federal Employees and Contractors (персональна перевірка особи федеральних співробітників та підрядчиків). Для виконання президентської директиви про внутрішню безпеку (HDSP-12) [1,2] в США були змушені створити технічну документацію, яка б надавала гарантії особи, що звернулася до системи з метою отримання доступу. Аналізуючи американський стандарт, виникає потреба у створенні моделі загроз, аналізі механізмів автентифікації з метою перекриття імовірних загроз, розвитку та впровадження систем контролю доступу. Але передусім необхідно зупинитися детально на проблемах автентифікації, а саме потрібно приділити увагу механізмам автентифікації, які використовують біометрику (фізичні характеристики або персональні поведінкові особливості, що використовуються для визначення особи або верифікації заявленої особи). Тому що використання як раз біометрики не тільки надає додаткові переваги до існуючих систем автентифікації, а й вносить додаткові проблеми.

1. ПРОБЛЕМИ АВТЕНТИФІКАЦІЇ

Насамперед проблеми автентифікації обумовлені технологією, яку використовує розробник при розробці програмного забезпечення PIV-картки. При використанні біометрики виникають такі складності: використовуючи динамічні біометричні дані, потрібно враховувати залежність фізичного та емоційного стану особи; біометричні дані не є секретними, оскільки люди залишають їх повсюди (наприклад, відбитки пальців); нечіткість відтворення (наприклад, поворот пальців на 30˚,60˚). В процесі вирішення цих проблем виникла ще одна – нерівномірний розподіл біометричної інформації, яка впливає на захищеність біометричного шаблону у випадку використання біометричної інформації у вигляді ключового матеріалу.

Для розроблення моделі загроз розглянемо базові механізми автентифікації PIV-карток.

2. МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ PIV-КАРТКИ

Залежно від рівня гарантії картка підтримує різні механізми автентифікації особи. Нижче приведено всі механізми, які розташовано за зростанням складності:

- *VIS* – механізм автентифікації, що ґрунтується на використанні візуальних посвідчень, як правило, підтримується для управління доступом до фізичних ресурсів та засобів;
- *CHUID* – механізм автентифікації, що ґрунтується на використанні унікального ідентифікатора утримувача картки, який доступний як з контактних, так і з безконтактних інтерфейсів;
- Механізм автентифікації з використанням біометричної автентифікації. В залежності від доступу поділяється на два типи:

– *BIO* – автентифікація на основі біометричної інформації без контролю зі сторони служби безпеки;

– *BIO-A* – автентифікація на основі біометричної автентифікації з контролем зі сторони служби безпеки (наприклад, за ходом автентифікації спостерігає інспектор або адміністратор з безпеки).

- *PKI* – механізм автентифікації з використанням асиметричних криптографічних перетворень.

3. МОЖЛИВІ ЗАГРОЗ

Аналіз зазначених механізмів автентифікації дозволяє визначити основні загрози. Механізми автентифікації та ідентифікації PIV-картки мають біометричну основу, тому аналіз механізмів необхідно проводити з урахуванням переваг та недоліків біометрики. До переваг слід віднести[2,3,4]:

- важкість фальсифікації біометричних шаблонів;

• висока достовірність біометричної автентифікації, в силу унікальності біометричних характеристик.

До недоліків слід віднести:

• залежність фізичного та емоційного стану особи, при використанні динамічних біометричних методів;

• не секретність біометричних даних (наприклад, кожна людина оставляє свої відбитки пальців, що надає змогу злочинцю підробити відбитки пальців);

Специфічність розгляду загроз автентифікації додає такі фактори: нечіткість відтворення біометричних даних та нерівномірний розподіл біометричної інформації.

Насамперед необхідно розглянути загрози, передбачені у національному законодавстві стосовно автентифікації особи. За результатами впливу на інформацію та систему її обробки, загрози можна поділити на такі:

• порушення конфіденційності інформації (отримання біометричної інформації користувачами або процесами всупереч встановленим правилам доступу);

• порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація біометричної інформації);

• порушення доступності інформації (часткова або повна втрата працездатності системи автентифікації, блокування доступу до інформації);

• втрата спостережливості або керованості системи обробки інформації (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень).

Також визначимося із основними шляхами здійснення загроз:

• технічні канали, які включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні та інші канали;

• канали спеціального впливу шляхом формування полів і сигналів з метою руйнування системи автентифікації або порушення цілісності інформації;

• шляхом підключення до апаратури та ліній зв'язку, маскування під реєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

При створенні моделі загроз автентифікації складемо перелік основних загроз та запропонуємо рекомендації щодо заходів для запобігання цих загроз в процесі автентифікації.

Взагалі загрози можна поділити на групи:

1. Основні:

• збої та відмови у роботі обладнання та технічних засобів АС;

• наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних);

• помилки персоналу (користувачів) АС під час експлуатації.

2. Випадкові:

• дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, даних, програм);

• ненавмисне пошкодження носіїв інформації;

• неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

• ненавмисне зараження ПЗ комп'ютерними вірусами;

• невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

• помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів;

• будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу;

• неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальних та ігрових програм, системного і прикладного ПЗ);

• випадковий підбір таємного біометричного шаблону на фізичному рівні;

• випадковий підбір електронного таємного біометричного шаблону;

• випадковий підбір криптографічного ключа чи довгого паролю;

• наслідки некомпетентного застосування засобів захисту.

3. Навмисні:

• порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

• порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції);

• компрометація таємного біометричного шаблону на фізичному рівні;

• перехват таємного електронного шаблону у вигляді його біометричних даних або у вигляді вектора його біометричних характеристик;

• перехват криптографічного ключа чи паролю;

• витягування конфіденційної інформації зі структури та параметрів перетворювача;

• саботаж та нелояльність користувача біометричної системи;

• порушення режимів функціонування АС (обладнання і ПЗ);

• впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

• використання засобів перехоплення побічних електромагнітних випромінювань і наведень, акустико-електричних перетворень інформаційних сигналів;

• використання (шантаж, змова; підкуп тощо) з корисливою метою персоналу АС;

• крадіжки носіїв інформації, виробничих відходів (роздруківок, записів);

• несанкціоноване копіювання носіїв інформації;

• читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

• одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

• неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку;

• впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж).

4. Потенційно можливі:

• навмисні зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як впливи (аварії, пожежа або інші навмисні події) на комутаційні вузли і канали передачі первинної мережі зв'язку;

• зміна умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони), такі як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, пожежі або затоплення приміщень унаслідок аварії інженерних комунікацій водопостачання;

• наслідки помилок при проектуванні і розробці компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних);

• помилки персоналу (користувачів) АС під час експлуатації обладнання і технічних засобів компонентів АС;

• невідповідна оцінка рівня захищеності, забезпеченого біометричним засобом високонадійної автентифікації;

• втрата доступності у випадку утрати та істотного викривлення біометричного шаблону легального користувача із-за травми, хвороби, прийому ліків, сп'яніння, струсу;

• навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів компонентів АС.

Переглянувши загрози, добрим тоном було би схематично змалювати модель загроз (рис. 1) [4].

Проаналізувавши та розглянувши наведені вище загрози від атак зловмисників та створену модель загроз, можна сформулювати декілька висновків: по-перше, атаки можуть бути виконані співробітниками або людиною, яка не працює в цій організації, хоча і в тому і в іншому випадку вони будуть в ролі зловмисника. По-друге, атаки можуть бути направлені на всю систему в цілому та кожний елемент окрема, на біометричні дані та результат механізмів автентифікації та ідентифікації. По-третє, зловмисників можна розрізнити по рівню підготовленості(володіння спеціальними навичками, програмним забезпеченням та обладнанням).

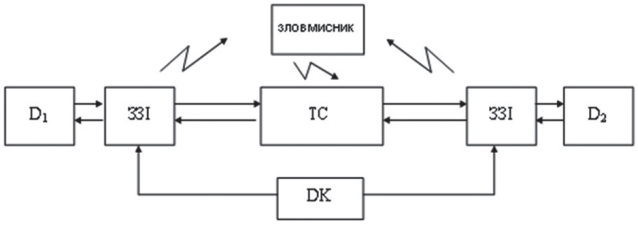

Рис. 1. Спрощена модель загроз

Узагальнюючи, можна сказати, що атаки зловмисника зможуть призвести до таких наслідків:

• Часткова або повна втрата працездатності системи автентифікації ;

• Некоректна робота системи автентифікації та ідентифікації;

• Порушення процедур автентифікації та ідентифікації користувачів та процесів надання їм повноважень;

• Неправильний результат процедури автентифікації та автентифікації користувачів;

• Отримання біометричної інформації користувачів всупереч встановленої політиці безпеки (правилам доступу);

• Повне або часткове знищення, викривлення, модифікація біометричної інформації .

РЕКОМЕНДАЦІЇ

З метою мінімізації або уникнення визначених загроз необхідно надати рекомендації щодо модернізації захисту системи. Насамперед потрібно врахувати декілька наступних напрямків захисту: обладнання, програмне забезпечення та особовий склад. У нашому випадку пропозиції та рекомендації будуть направлені на підвищення стійкості механізмів автентифікації та ідентифікації системи, які використовують біометричні методи:

– спираючись на досвід розвинутих країн — ввести розмежування доступа (фізичного та електронного доступу);

– створення механізмів автентифікації та ідентифікації відповідно до доступу (біометричної ідентифікації під наглядом та без нього, захист на рівні програмного забезпечення(криптографія-криптографічні протоколи));

– створенні механізми автентифікації повинні бути в межах 5 класів автентифікації (0-4 класи) (див. табл. 1);

– налагодження політики безпеки в ІТС відповідно до рівнів доступу (на самій ЕОМ);

– використання обладнання, сертифікованого в Україні;

– використання обладнання, як для перевірки картки пред'явника, так і перевірки (ідентифікації) особи власника картки (сканери, зчитувачі);

– налагодження чутливості обладнання (пристроїв зчитування) — для вирішення проблем 1 та 2 роду;

– використання посвідчення (картки контролю доступу власника);

– в залежності від потреби (який рівень гарантії хочуть отримати власники) та кількості користувачів у системі потрібно визначити біометричний метод та потрібно враховувати такі фактори та характеристики:

– швидкість отримання відповіді;

– розміри обладнання(габаритність);

– економічний фактор;

– імовірність справжності особи (помилки 1-го та 2-го роду).

Таблиця 1

Клас 0	Незахищений
Клас 1	Захищений від розкриття заявленої ІА
Клас 2	Захищений від розкриття заявленої ІА й атаки типу «повтор» для різних перевірників
Клас 3	Захищений від розкриття заявленої ІА й атаки типу «повтор» на одного перевірника
Клас 4	Захищений від розкриття заявленої ІА й атаки типу «повтор» на одного перевірника або різних перевірників

Рекомендації були зроблені на основі розгляду сучасних нормативних документів, стандартів та використанні сучасних методів та технологій. Зважаючи на вищевикладене, головна мета створення системи захисту з використанням біометрики зводитися до вибору оптимальних характеристик та показників компонентів системи.

Література:

[1] FIPS PUB 201.Personal Identity Verification (PIV) of Federal Employees and Contractors. 2006

[2] HDSP-12. Homeland Security Presidential Directive 12.2003

[3] ГОСТ Р 52633-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

[4] *Горбенко І.Д., Горбенко Ю.І.* Інфраструктура відкритих ключів. Електронний цифровий підпис.Теорія та практика: монографія. – Харків: Видавництво "Форт", 2010. – 608с.

Надійшла до редколегії 16.05.2011

Балагура Дмитро Сергійович, доцент кафедри Безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, криптографічні протоколи вироблення та узгодження ключів.

Іваненко Дмитро Вікторович, аспірант кафедри Безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, методи та засоби автентифікації даних.

УДК 681.3.06

Основные аспекты защищенности механизмов аутентификации PIV-картки / Д.С. Балагура, Д.В. Иваненко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 255–258.

В данной статье изложены результаты анализа угроз механизмов аутентификации, была предложена модель угроз и требования к ней, были даны рекомендации по перекрытию вероятных угроз.

Ключевые слова: угроза, аутентификация,модель угроз, биометрика, рекомендации.

Табл. 01. Рис. 01 Библиогр.: 04 назв.

UDC 681.3.06

Basic aspects of the security of PIV-card authentication mechanisms / D.S. Balagura, D.V. Ivanenko // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 255–258.

This paper presents the results of authentication mechanisms threat analysis and proposes a model of threats and requirements for it. Recommendations to eliminate possible threats are given in this paper.

Keyword: threat, authentication, threat model, biometrics, recommendations.

Tab. 01. Img. 01 Ref.: 04 items.