УДК 621.391

Р.Б.Стахів, УАД, м.Львів

МЕТОДИ ВИЗНАЧЕННЯ РІВНЯ БЕЗПЕКИ ПРОДУКЦІЇ, ЩО ВИКОРИСТОВУЄ ЗАСОБИ ЗАХИСТУ ЕТИКЕТОК

Досліджуються методи визначення рівня безпеки продукції, захищеної етикетками та можливості вибраних типів атак по підробці, або фальсифікації засобів захисту та неавторизованому використанні оригінальних засобів захисту.

The methods of determination of strength of products, protected labels and possibilities of the chosen types of attacks on an imitation security are probed, or falsification of facilities of defence and unauthorized use of original facilities of defence.

Вступ

Використання етикеток, незалежно від акцентів такого використання, завжди передбачає забезпечення тієї, чи іншої міри безпеки. Навіть у випадку, коли основною ціллю її використання приймається рекламування відповідного товару, тоо факт розміщення такої етикетки на відповідному продукті обумовлює ефект захисту товару від леяких типів атак.

Параметр, що характеризує рівень захисту, в даному випадку товару, або рівень безпеки, необхідно обчислювати, оскільки визначати його величину на двійковій множині значень не коректно.

В даному випадку, під терміном захист розуміється деяка властивість одного елемента або компоненти, що орієнтована на забезпечення захисту і залежить від типу атаки та типу елемента захисту, а термін безпека означає деякий рівень можливостей протидіяти довільним типам атак певної сукупності засобів захисту, які складають систему безпеки. У зв'язку з цим, в статті рівень безпеки системи будемо визначати на основі даних про рівні захисту, які забезпечують окремі засоби захисту, що використовуються в рамках захисту продукту.

Дослідження рівня безпеки і атак на етикетки

Розглянемо окремий засіб захисту, який представляє собою деякий графічний образ, переважно, абстрактний типу узору. Вибір графічного образу типу узору обумовлений тим, що узор представляє собою деяку впорядковану структуру, яка описується певними параметрами, які можна повязати з механізмами протидії атакам на відповідну етикетку і безпосередньо на окремий засіб захисту. Таким чином, говорити про можливості протидії атакам окремих засобів захисту можна тільки у тому випадку, якщо відповідні атаки є відомими.

Проблеми захисту і, відповідно, безпеки можна розглядати з точки зору наступних підходів:

А) на основі даних про можливі атаки та про методи дії таких атак на обєкти, що захищаються, будуються засоби захисту, функції яких полягають у наступному:

- виявленні атак,
- протидії впливу, що реалізується атакою на обєкт, або на продукт,
- протидії наслідкам впливу атаки на продукт,

Б) на основі даних, які, в загальному, оцінюють можливість виникнення атак та можливі типи атак, які мають характер ймовірнісних подій і на їх основі реалізується наступне:

- вибір необхідних засобів захисту, що орієнтовані на найбільш ймовірні атаки,
- ідентифікація типу атаки, що була виявлена вибраними засобами захисту,
- у відповідності до типу атаки, активізується необхідний засіб захисту.

В) вибираються типи атак, що відповідають типам етикеток, засоби захисту вибираються у відповідності до вибраних типів атак, які реалізують кроки аналогічні тим, що виконуються у випадках а) і б), при цьому, враховується специфіка цього підходу.

До атак, які можуть активізуватися по відношенню до етикеток, можна віднести досить малу кількість їх різновидностей. Відповідні атаки тісно повязані з засобами захисту, що використовуються ветикетках. По суті, формування атак проводиться на основі даних про ті, чи інші засоби захисту і чим більше у небезпеки даних про засоби захисту, тим більш ефективною буде атака, оскільки в способі її реалізації враховуються можливості відповідного засобу захисту. В даному випадку, обмежимося засобами захисту, що представляють собою абстрактні графічні образи типу узорів.

Атаки, що реалізуються по відношенню до етикетки, можна розділити на наступні типи:

- підробка засобу захисту, при не авторизованому виготовленні етикетки,
- заміна засобу захисту на інший, графічно подібний на оригінальний засіб,
- використання етикетки разом з засобами захисту до продукту, який відноситься до того ж класу, що і оригінальний продукт, але у якого персональні параметри не відповідають продукту, для якого використовується етикетка.

Виходячи з приведених типів атак, можна стверджувати, що більшість атак полягає у підробці, або фальсифікації засобів захисту та у неавторизованому використанні оригінальних засобів захисту. Оскільки, різні атаки орієнтовані на використання їх по відношенню до етикеток різного типу, то необхідно розглянути специфіку дії таких атак на відповідні етикетки.

Дія атак на етикетку типу E^V полягає у підміні товару, для якого використовується етикетка, яка відповідає іншому товару. В цьому випадку,

оригінальний і не оригінальний товари відрізняються персональними параметрами $p_{p(j),k}$. Таким чином, реалізується порушення безпеки товару, оскільки товар описаний на етикетці не відповідає товару, який такою етикеткою ідентифікується. Переважно товар, яким підміняється продукт описаний на етикетці, є товаром нижчої якості по відношенню до оригінального товару. В протилежному випадку така атака була би не обгрунтована, оскільки, якісний товар є дорожчий від товару менш якісного.

Для атак на етикетку типу E^T, що орієнтована на захист авторських прав, полягає у використанні підроблених етикеток для маркування продукту, який виготовлений у відповідності з авторською технологією виробником, який не має авторських прав на використання таких технологій. В цьому випадку, продукт по своїх параметрах відповідає авторському, а етикетка є фальшивою, оскільки для того, щоб отримати авторські етикетки, необхідно мати авторські права на виготовлення відповідного продукту, або сертифікат на цей технологічний процес.

Дія атак на етикетку типу E^C, що орієнтована на захист споживачів продукту, полягає у тому, що для маркування товару не залежно від того, чи цей товар є авторським, чи ні, використовується фальшива етикетка з підробленими засобами захисту та фальшивими даними по продукт.

Дія атак на етикетку типу E^R полягає у тому, що використовується фальшива етикетка із зміненими рекламними даними, які суперечать параметрам, що описують продукт. При цьому, така суперечність, в першу чергу, стосується персональних параметрев продукту.

Дія атак на етикетку типу E^A полягає у тому, що використовується фальшива етикетка, яка описує не властиві для цього продукту параметри його дистрибуції. При цьому, засоби захисту можуть бути оригінальними.

Для того, щоб можна було говорити про систему безпеки продукту, що грунтується на використанні етикеток, необхідно прийняти наступні положення:

- функції захисту реалізуються в цілому етикеткою, яка складається з окремих функціональних компонент, що розміщаються на етикетці, до яких відносяться наступні:
- спеціальні графічні засоби захисту (Z^G),
- фізичні засоби захисту, що можуть розміщатися на етикетці та можуть мати різну природу (Z^Φ),
- т екстові компоненти, що описують параметри продукту, що ідентифікується етикеткою, що дозволяє в певній мірі їх ідентифікувати, як засоби захисту (Z^D),
- текстові компоненти, що ідентифікують дані про продукт, які орієнтовані на споживача, що, як і у попередньому випадку, дозволяє їх інтерпретувти як засоби захисту (Z^C),
- текстові компоненти, що представляють собою рекламні дані і також можуть допускати свою інтерпретацію як засоби захисту (Z^R),

- текстові дані, що описують особливості дистрибуції відповідного товару і також інтерпретуються як засоби захисту (Z^A).

Наступною моделлю, яка включається в в загальну модель етикетки, є модель безпеки продукту, яку можна описати у вигляді наступного співвідношення:

$$BM^E = F^B[Z^G, Z^\Phi, Z^D, Z^C, Z^R, Z^A]. \quad (1)$$

Компоненти, що входять в BM^E, можна розділити на наступні групи засобів захисту:

- графічні засоби захисту Z^G,
- фізичні засоби захисту Z^Φ,
- текстові засоби захисту $Z^T := (Z^D, Z^C, Z^R, Z^A)$.

Про графічні засоби захисту неодноразово згадувалось вище. Прикладом фізичних засобів захисту можуть служити голограми, перфорації та різні фізичні включення, які широко використовуються в системах безпеки документів [1].

Текстові засоби захисту представляють собою тексти, що описують семантику, яка відображає різну тематичну спрямованість відповідного тексту. Текстові фрагменти відносяться до засобів захисту завдяки тому, що в рамках текстової інформації можуть укриватися різними стеганографічними методами додаткові дані, які від етикетки і, відповідно, від однієї партії продукту до іншої можуть змінюватися у відповідності до певного алгоритму. Наприклад, якщо укритими даними є деяке число, то останнє може представляти собою криптограму, розшифрування якої потребує знання відповідного ключа. В цьому випадку, виникає можливість для захисту етикеток та, відповідно, продукту можна використовувати криптографію [2].

Текстові записи на етикетці можуть служити засобами захисту не тільки завдяки використанню стеганографічних методів, а і завдяки використанню семантичних методів. Суть цих семантичних методів полягає у наступному. Текстова інформація, що розміщається на етикетці, не відповідає тільки одному типу етикетки, а формується таким чином, щоб текст на етикетці відповідав потребам типу E^R, E^T, E^C, E^V і в багатьох випадках E^A. Кількість текстової інформації, що відповідає різним типам є різна, але це не означає, що ця інформація може бути не узгоджена між собою особливо, коли мова йде про фрагменти, що стосуються рекламної інформації.Оскільки, рекламна інформація стосується характеристик продукту та стосується даних, які визначають міру приязності продукту для споживача, то семантична узгодженість є важливим параметром, який може бути виміряний кількісно. В цьому випадку, величина семантичної узгодженості використовується як параметр захисту, оскільки, спосіб її визначення відомий тільки виробнику, а його значення залежить від семантичних словників, які є доступними тільки для виробника продуктів. Слід відзначити, що тип етикетки, що визначається характером текстової інформації, яка на ній друкується, визначається величиною семантичної значимості тексту, який на ній друкується і також

визначає тип етикетки. Оскільки, на етикетці розміщаються всі типи текстів, то процент величини тексту, семантична значимість якого є найвища, визначає тип етикетки. Необхідність визначати тип етикетки по величині семантичної значимості цього тексту, а не по самій величині тексту, чи розмірах, або місцях розміщення тексту на етикетці обумовлюється тим, що розмір тексту може бути великим, але вплив цього тексту на споживача може бути не значним. Те саме може стосуватися і місця розміщення того, чи іншого тексту.

Перш ніж проводити аналіз моделі безпеки в цілому, необхідно зауважити, що розглядати систему безпеки захисту тільки в рамках засобів захисту, що розміщаються на етикетці, не доцільно. Необхідно в цю систему включати всі стадії функціонування продукту, до яких відносяться стадія, або етап дистрибуції продукту, яка включає його зберігання на складах та стадія продажі продукту. на якій споживач безпосередньо приймає рішення про доцільність його використання і здійснює його покупку. На цьому етапі функціонування продукту не закінчується, оскільки, особливо, для продуктів промислових існує етап обслуговування експлуатації, або споживання, в рамках якого можуть виникнути процеси рекламації та процеси підтвердження заявленого рівня якості продукту, якщо мова йде про продукти споживання. В загальному, ці етапи будемо називати етапом дистрибуції та етапом споживання. Якщо етап дистрибуції обслуговується додатковими документами, які виконують функції ідентифікації товарів і тим самим в певній мірі реалізують захисні функції, то етап використання продукту потребує додаткового аналізу.

Етап використання для споживчих продуктів складається з етапу покупки та споживання. Серед засобів захисту, що розміщаються на етикетці, можна виділити наступні типи, які безпосередньо повязані з типами атак. Одна з найпоширеніших атак полягає у використанні фальшивих етикеток. В цьому випадку, захист полягає у виявленні фальшивих етикеток. Найбільш актуальною процедурою виявлення фальшивих етикеток реалізується на етапі покупки товару споживачем. На цьому етапі забезпечити еквівалентні мірі захищеності можливості для перевірки етикеток є найбільш складно. Ця складність зростає зі складністю розпізнавання авторського походження відповідного засобу захисту. Для ідентифікації засобу захисту в оперативному режимі, що є характерним для споживача. Коли він повинен прийняти рішення про придбання відповідного продукту, необхідно надавати йому засоби автоматичної ідентифікації, які моглиб з достатньою мірою достовірності таку ідентифікацію провести. Оскільки, для масових споживачів продуктів не надається така можливість, то існує процедура рекламації, яка може подаватися покупцем у випадку порушення безпеки шляхом підміни продукту контрафактом. В рамках цієї системи безпеки, яка включає всі засоби захисту, що розміщаються на етикетці, та системи дистрибуції, рівень безпеки, який визначається окремими графічними засобами захисту, повинен бути співвимірним з можливістю адекватного

використання цих засобів, в першу чергу, споживачем.

При реалізації відповідного забезпечення етапу продажі, засобами ідентифікації компонент, що орієнтовані на захист продукції, рівень безпеки на всіх етапах функціонування продукту буде визначатися рівнем захисту, який забезпечують засоби захисту, що використовуються в етикетках.

Для засобів захисту, що представляють собою графічні образи, які представляють собою правильні узори, захист полягає у порівнянні даного фрагмента узору з еталоном, або у перевірці параметрів графічних образів на їх відповідність заданим значенням. Такі параметри змінюються для кожної партії продуктів, що приводить до підвищення рівня захищеності.

Засоби захисту, що визначаються текстовими фрагментами полягають у побудові текстів, які мають задані значення семантичних параметрів [3]. Такі семантичні параметри формуються між текстами фрагментів, що мають різну функціональну орієнтацію.

Для формування способу оцінки рівня захищеності, необхідно розглянути наступні задачі:

- визначити зовнішні ознаки, що визначають необхідний рівень захищеності продукту,
- вибрати параметри засобів захисту, значення яких можна вимірювати,
- визначити способи вимірювання значень параметрів засобів захисту,
- сформувати техноглогію використання засобів захисту,
- сформувати правила управління мірою захисту.

Оскільки джерелом атак на системи захисту продуктів в більшості випадків є зовнішні небезпеки, то необхідно визначити та обгрунтувати зовнішні параметри, що характеризують міру необхідності використання захисту продукції. Очевидно, що більшість спроб порушити авторські права, чи фальсифікувати продукт повязані з отриманням не обгрунтованого прибутку. Тому, приймемо, що на міру захисту, яку повинні забезпечувати засоби захисту, впливають наступні зовнішні фактори:

- масовість продукції (m_i),
- розміри продуктів, що захищаються (r_i),
- вартість окремих продуктів (v_i).

Приймемо, що міра захищеності η, для масової продукції прямо пропорціонально залежить від масовості продукції, обернено пропорціональна до вартості продукції та залежить від розмірів окремого продукту. Для прикладу, зупинимося на продовольчих товарах. Тоді, для міри захищеності можна записати :

$$\eta^m = \alpha m_i r_i / v_i, \qquad (2)$$

де α - коефіцієнт пропорціональності. Очевидно, що це співвідношення є вірним тільки для певних діапазонів значень параметрів m_i та v_i. Величина m_i визначається потенціальною кількістю споживачів. Для прикладу, можна прийняти, що величина v_i росте із зменшенням r_i. Така залежність визначається характером продукту, який буде визначатися його собівартістю.

Для продукту собівартість якого є велика, залежність для η можна записати у вигляді наступного співвідношення:

$$\eta^R = (v_i.r_i)/(R^{tp} \cdot m_i), \quad (3)$$

де R^{tp} – рівень автоматизації процесу виготовлення, величина якого змінюється в діапазоні [1,∞] , де $minR^{tp}$=1. Приведені співвідношення носять імпіричний характер і відображають загальні тенденції взаємозвязків небезпек з відповідними продуктами. Формули типу (2) і (3) можуть використовуватися для початкової оцінки необхідного рівня захисту відповідних товарів. В процесі виробництва, дистрибуції і споживання товарів вимоги до значення величини η можуть змінюватися. Такі зміни можна відслідковувати наступними способами:

- аналіз та оцінка ймовірності наявності та кількості контрафакту відповідного продукту на ринку,
- перерахунком величин, що входять у формули (2) і (3) у випадку зміни параметрів v_i, r_i, R^{tp}, m_i,
- збільшення, або модифікація кількості параметрів, що використовуються у співвідношеннях для η.

Найбільш адекватний спосіб визначення необхідного рівня безпеки, який необхідно забезпечувати. Для продукту, грунтується на моніторуванні атак, що реалізуються на відповідний продукт в процесі його виробництва, дистрибуції та споживання. В цьому випадку, у власника продукту накопичуються дані про атаки на продукт і на основі таких даних можна спрогнозувати активність небезпек на певний період часу, а також можна прогнозувати типи атак, що дозволить провести адекватну модифікацію засобів захисту та модифікацію системи безпеки в цілому.

Розглянемог способи вимірювання текучого рівня безпеки. Очевидно, що рівень безпеки продукту не етапі виробництва в межах однієї партії є постійним, якщо його оцінювати по відношенню до засобів захисту, що розміщаються на етикетках. Тому, коли йде мова про збільшення чи зменшення рівня безпеки, то в цьому випадку рівень безпеки визначається на основі даних про загальну кількість атак на продукт та кількість атак, які були виявлені, оскільки сама етикетка, як засіб захисту, ніяких дій активізувати не може у відповідь на атаку, що виникає. Тому, детальніше розглянемо уявлення про протидію атаці на продукт, що захищається етикеткою.

Приймемо, що атака на продукт в кінцевому випадку, завжди може бути виявлена, оскільки, в рамках системи безпеки передбачається періодичний лабораторний аналіз продукту, який відбирається для аналізу на етапі продаж. В цьому випадку, виявляється атака на фальсифікацію продукту. Крім аналізу продукту, проводиться аналіз засобів захисту, які розміщені на етикетці, таким чином, виявляється атака на порушення авторських прав. Крім того, проводиться перевірка всіх засобів захисту, які використовуються на етапі дистрибуції, до яких відноситься документація, що супроводжує продукт, яка

має власні засоби захисту, та перевіряються засоби, що забезпечують ідентифікацію продукції при її зберіганні та транспортуванні. Оскільки всю продукцію перевірити не можливо, то все, що підлягає контролю вибирається у відповідності з певним правилом, що визначає випадковість відповідного вибору. Атаки, які були виявлені на етапі перевірок, які будемо називати аудитом системи безпеки, як це прийнято називати в системах безпеки, представляють собою атаки, які ми будемо відносити до успішних атак [4]. Всі атаки, які виявлені в періоди між проведенням аудиту, будемо відносити до атак, які виявлені завдяки системі безпеки, що складається з засобів захисту,, які розміщаються на етикетці, засобів захисту, що обслуговують етап дистрибуції та засобів захисту, що обслуговують процеси продажі. Введемо наступні визначення атак.

Визначення 1. Атака at_i називається виявленою, якщо вона виявлена на етапі дистрибуції, чи на етапі продажі учасниками цих процесів в проміжку інтервалів проведення аудиту системи безпеки.

Формально, кількість виявлених атак системою захисту можна описати наступним співвідношенням:

$$at_i^V = \sum_{j=1}^{m}[t_j = Sg(T\ mod\ \Delta T)],$$

де T - текуче значення часу, ΔT - період проведення аудиту, at_i^V - виявлена атака, t_j - момент виникнення атаки.

Визначення 2. Атака at_i називається не виявленою, або успішною, якщо вона розпізнана в момент проведення аудиту системи безпеки.

Формально, кількість атак at_i^U можна описати наступним співвідношенням:

$$at_i^U = \sum_{j=1}^{m}[t_j = \urcorner Sg(T\ mod\ \Delta T)],$$

де t_j - момент виявлення атаки в процесі реалізації аудиту системи безпеки.

Тепер можна визначити рівень безпеки системи захисту наступним чином:

Визначення 3. Рівень безпеки rb_i, який забезпечує система захисту продукту, визначається співвідношенням кількості виявлених атак до суми атак, що були здійснені за період часу її функціонування рівний ΔT.

Формально, це можна описати наступним співвідношенням:

$$rb_i(\Delta T_i) = at^V(\Delta T)/[at^V(\Delta T) + at^U(\Delta T)]. \quad (4)$$

Виходячи із співвідношення (3.9) видно, що рівень безпеки системи захисту змінюється від нуля до одиниці. Величина rb_i=0, коли ні одна атака не була виявлена, а всі атаки, що сталися, виявилися успішними. Величина rb_i=1, коли всі атаки на продукт були виявлені в процесі одного циклу функціонування системи безпеки (SB).

З ряду величин $rb_1(\Delta T_1)$, $rb_2(\Delta T_2)$, …, $rb_n(\Delta T_n)$ можна побудувати функцію зміни величинирівня безпеки в залежності від часу функціонування системи SB. На основі даних $\{rb_1(\Delta T_1),\ rb_2(\Delta T_2),\ \ldots,\ rb_n(\Delta T_n)\}$, які відповідають моментам часу $\{t_1, [(t_1 + \Delta T) = t_2], \ldots, t_1, [(t_{n-1} + \Delta T) = t_n]\}$, можна побудувати многочлен, наприклад, Гауса, який інтерполює відпвідні

значення rb_i, що можна записати у наступній формі [5]:

$$P(x) = \sum_{i=1}^{n+1} f(x_i) P_i(x_i), \quad (5)$$

де $f(x_i) = P(x_i)$, де $P(x_i)$ – інтерполяційний многочлен, що інтерполює функцію $f(x_i)$ у вузлах інтерполяції.

Висновок

На основі використання інтерполяційного многочлена $P(x) = a_o + a_1 x_1 + a_2 x_2 + \cdots + a_m x_m$ можна розвязувати задачу екстраполяції функції $f(x_i) = rb(t_i)$, що представляє собою задачу прогнозування значення функції на момент часу $t_{n+1} = t_n + \Delta T$. Таким чином, стає можливим визначити величину рівня безпеки функції $rb_i(t_i)$, що найменше на інтервалі часу ΔT.

1. *Шевчук А.В., Музика В.П.* Виготовлення та захист вітчизняних паспортних документів. // Друкарство, 2003, N5(52).
2. *Бернет С., Пэйн С.* Криптография. Официальное руководство RSA Security. М.: Бином-Пресс, 2002.
3. *Афанасьева О.Ю., Дурняк Б.В., Коростіль О.Ю.* Методи відображення технічних параметрів образів в семантичному словнику стеганосистеми./ Збірник наукових праць, ІПМЕ НАН України, Київ, 2007, вип. 38.
4. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001.
5. *Зельдович Я.Б., Мышкис А.В.* Элементы прикладной математики. М.: Наука, 1972.

Поступила 18.03.2013р.