Сучасний стан наукових досліджень та технологій в промисловості. 2024. №3 (29)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.9
DOI: https://doi.org/10.30837/2522-9818.2024.3.057

О. Пономаренко, В. Горбачов

МЕТОД ОБФУСКАЦІЇ ПРОЄКТУ ЕЛЕКТРОННИХ СИСТЕМ НА ОСНОВІ АГРЕГАЦІЇ

Під час виготовлення інтегральних схем існує ймовірність додавання апаратних троянів на будь-якому етапі циклу розроблення. Атаки апаратних троянів пов'язані зі зловмисними модифікаціями інтегральних схем у процесі проєктування або виготовлення, де залучаються ненадійні інструменти проєктування або компоненти. Такі модифікації можуть призвести до небажаної поведінки інтегральних схем або до появи прихованих каналів витоку інформації. Існують різні методи класифікації, виявлення та запобігання додаванню апаратних троянів. Одним із таких підходів є проєктування на основі обфускації, що ґрунтується на приховуванні функціональних та структурних властивостей проєкту, що ускладнює для зловмисника додавання троянів. **Предметом дослідження** є метод обфускації проєкту електронних систем на основі агрегації. **Мета роботи** – дослідження процесу обфускації проєкту електронних систем на основі агрегації. Ключова ідея полягає в тому, що етап розроблення та під'єднання монітору безпеки виконується в надійному середовищі. Отже, зловмисник не зможе отримати його функціональність та оригінальну структуру. **Актуальність роботи** полягає в тому, що зазначений підхід запобігає можливості функціонування апаратних троянів. У статті передбачається розв'язання таких **завдань**: розроблення та дослідження алгоритму обфускації проєкту електронних систем на основі агрегації; реалізація подання монітору безпеки як окремої підсистеми, пов'язаної з основним проєктом; експериментальне оцінювання можливостей методу. **Результати роботи**: продемонстровано метод обфускації проєкту електронних систем на основі агрегації; запропоновано монітор безпеки як окрема підсистема, що пов'язана з основним проєктом; виконано експериментальне оцінювання можливостей методу. **Висновки**. Підхід для проєктування на основі обфускації полягає в тому, що інтегральна схема модифікується, отже, приховуються функціональні та структурні властивості проєкту, що ускладнює для зловмисника додавання троянів. Обфускація на основі агрегації полягає в тому, що монітор безпеки розглядається як окрема підсистема, пов'язана з основним проєктом.

Ключові слова: апаратна безпека; обфускація проєкту електронних систем; монітор безпеки; агрегація.

Вступ

Апаратні трояни пов'язані зі зловмисними модифікаціями інтегральних схем (ІС) та вони можуть бути додані в ІС на будь-якому етапі циклу її розроблення. Такі модифікації можуть призвести до появи прихованих каналів витоку інформації або до небажаної поведінки ІС [1].

У роботі [2] стверджується, що такі етапи, як специфікація, тестування пакетів і розгортання, не вразливі до додавання апаратних троянів. Інші етапи, наприклад проєктування та виготовлення, вразливі до атак безпеки, та підтримання жорсткого контролю над циклом розроблення проєкту ІС є дуже дорогим. На цей час вже існує чимало різних методів виявлення та запобігання додаванню апаратних троянів (класифікація наведена в [3, 4]).

Обфускація проєкту є методом запобігання крадіжці інформації, зворотній інженерії, клонуванню та незаконному використанню ІС [5]. Підхід для проєктування на основі обфускації ґрунтується на приховуванні функціональних і структурних властивостей проєкту, що ускладнює для зловмисника додавання троянів [1]. Обфускація є рішенням для захисту інтелектуальної власності електронних систем від таких атак, як зворотна інженерія та піратство [6]. За останнє десятиліття було розроблено чимало методів обфускації електронних систем.

У процесі обфускації електронних систем специфікація проєкту шифрується, змінюється опис або структура ІС та навмисно приховується її функціональність. Отже, результуюча архітектура стає неочевидною для зловмисника, що ускладнює піратство.

Ця робота присвячена дослідженню методу обфускації проєкту електронних систем на основі агрегації. Розв'язуються такі завдання: розроблення та дослідження алгоритму обфускації проєкту електронних систем на основі агрегації; реалізація подання монітору безпеки як окремої підсистеми, пов'язаної з основним проєктом; експериментальне оцінювання можливостей методу.

Аналіз літератури

Апаратні трояни можуть бути додані в ІС на будь-якому етапі циклу її розроблення. Атаки

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 3 (29)

апаратних троянів стали основною проблемою безпеки інтегральних схем [1]. Ці атаки пов'язані зі зловмисними модифікаціями ІС під час проєктування або виготовлення в ненадійному проєктному центрі чи на виробництві, де залучаються ненадійні люди, інструменти проєктування або компоненти [1].

Були запропоновані методи класифікації апаратних троянів на основі різних характеристик [2]. Існує така класифікація: комбінаційні – активація троянів залежить від виникнення конкретної умови на певних внутрішніх вузлах схеми; послідовні – активація троянів залежить від появи якоїсь послідовності логічних значень у внутрішніх вузлах [2].

Деякі класифікації основані на механізмах активації (*Trojan trigger*) та частині схеми або функціональності, на які впливає активація трояна (*Trojan payload*) [2]. Детальна класифікація апаратних троянів наведена в роботі [2].

Існують такі підходи виявлення троянів: логічне тестування та аналіз сторонніх каналів [1]. Логічне тестування полягає у розробленні тестових шаблонів для виявлення трояна. Такий підхід, найімовірніше, не зможе активувати великі трояни, що містять значну кількість тригерних входів [1].

Іншим підходом є вимірювання параметра стороннього каналу, наприклад, затримки шляху, на який можуть вплинути ненавмисні модифікації конструкції. Але ефективність аналізу сторонніх каналів обмежена великими варіаціями внутрішніх параметрів пристрою в сучасних технологіях [1]. Рішення, що поєднує в собі переваги обох підходів, може бути використано для виявлення троянських програм різних типів і розмірів [1].

Підходи, що запобігають додаванню троянів, поділяють на дві категорії: підходи на основі обфускації та підходи із заповненням макета. Підходи на основі обфускації ґрунтуються на приховуванні функціональних та структурних властивостей дизайну, що ускладнює для зловмисника додавання троянів [1].

Підходи із заповненням макета спрямовані на те, щоб позбутися можливості долучення додаткових компонентів схеми в проєкт способом заповнення вільного простору. Такий підхід ускладнює для зловмисника пошук місця на пристрої з метою додавання троянів [1].

Існують три типи обфускації електронних систем: пасивна обфускація, активна обфускація та обфускація на основі реконфігурованої логіки [5]. Схеми активної обфускації електронних систем можна поділити на обфускацію на основі комбінаційної логіки і на основі скінченного автомата (СА).

- У разі пасивної обфускації електронних систем опис проєкту шифрується за допомогою криптографічних методів перед тим, як передати його до ненадійних етапів циклу створення ІС. Розробник надає клієнтам правильний ключ для розшифрування проєкту [5].
- Активна обфускація полягає в модифікації функціональності ІС для захисту проєкту від зворотної інженерії, клонування та створення більшої кількості копій ІС, ніж було замовлено [5].
- Обфускація на основі комбінаційної логіки модифікує проєкт способом включення додаткових логічних вентилів [5].
- За умови обфускації на основі СА модифікується проєкт схеми та блокується кожна ІС за допомогою унікального шляху переходу стану [5].
- Обфускація на основі реконфігурованої логіки використовує функції реконфігурації ІС для обфускації проєкту. Підхід полягає в тому, щоб зробити невеликий компонент проєкту реконфігурованим в ІС. Отже, приховуються функціональні та схемні деталі на ненадійних етапах циклу розроблення [5].

Підходи до проєктування захищеної системи мають бути основані та таких чинниках:

1) формальних моделях безпеки, що забезпечують стійкість системи до несанкційного доступу, в умовах виникнення в її компонентах зловмисних вторгнень;

2) сучасних методах проєктування захищеної системи, що передбачають наявність механізму безпеки як обов'язкового елемента;

3) теоретично обґрунтованих гарантіях безпеки системи;

4) застосуванні математичного моделювання для оцінювання теоретичних результатів, що стосуються безпеки систем [7], [8].

Концепція монітора безпеки (МБ) – механізму контролю доступу – є базовою в проєктуванні та розробленні захищених систем [9]. МБ є концепцією контролю доступу абстрактної машини, що опосередковує всі доступи суб'єктів до об'єктів [10]. Завдяки МБ розробники можуть додати аспект безпеки в процес проєктування системи замість того, щоб намагатися долучити його пізніше. Абстрактна модель МБ може застосовуватися до будь-якого типу системи, яка потребує забезпечення контролю доступу [11].

Перелічимо властивості монітора безпеки відповідно до праці [12]:

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №3 (29)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

• МБ має бути таким, щоб його неможливо було обійти, зокрема зловмисник не міг обійти механізм контролю доступу й порушити політику безпеки;

• МБ має бути захищеним від несанкційного доступу, оскільки в іншому разі зловмисник може руйнувати сам механізм і таким чином порушити політику безпеки;

• МБ має піддаватися оцінюванню, тобто аналізу та тестам, повнота яких може бути гарантована. В іншому разі механізм, імовірно, матиме недоліки, через які політика безпеки не виконуватиметься;

• МБ має завжди викликатися, оскільки без цієї властивості механізм може не працювати в той момент, коли це буде потрібно, через що зловмиснику вдасться порушити політику безпеки.

У цій статті розглядається обфускація на основі реконфігурованої логіки на стадії після виготовлення ІС, а також порушується питання необхідності додавання етапу реконфігурованої логіки до циклу розроблення. Цей підхід допомагає приховати частину проєкту від зловмисника, а саме функції та структуру мікросхеми доти, доки не буде запрограмована реконфігурована логіка. Обфускація на основі реконфігурованої логіки дає змогу розрізняти розроблення та виробництво ІС. Отже, проєкт можна майже повністю розробити в надійному середовищі, за винятком деяких периферійних функцій, доданих до основних елементів.

Обфускація монітора безпеки на основі агрегації

У цій статті демонструється метод обфускації проєкту електронних систем на основі агрегації, який полягає в тому, що приховується під'єднання МБ, щоб зловмисник не міг отримати його функціональність та оригінальну структуру.

Розглянемо цей метод детальніше.

Елементи системи S об'єднуються в підсистеми S_μ, де $\mu = 1,\ 2, ..., M$. Якщо підсистема $S\mu$ є складною, тоді вона має зовнішнє середовище. Зовнішнє середовище позначається як фіктивний елемент C_0^μ або підсистема $S_{\mu 0}$ [13], [14].

Підсистема S_μ, пов'язана із зовнішнім середовищем, зображена на рис. 1.

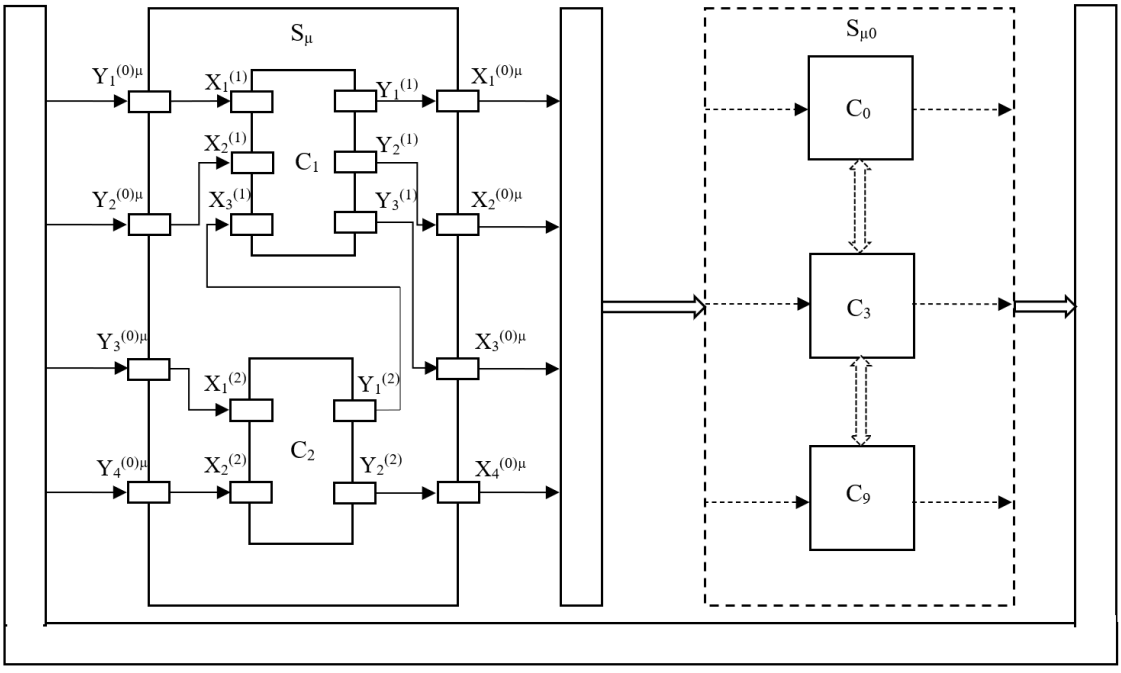

Рис. 1. Підсистема S_μ, пов'язана із зовнішнім середовищем

Взаємодія між підсистемою S_μ та зовнішнім середовищем здійснюється завдяки вхідним контактам $X_i^{(0)\mu}$ зовнішнього середовища, що з'єднуються з вихідними контактами елементів підсистеми S_μ, та за допомогою вихідних контактів $Y_l^{(0)\mu}$ зовнішнього середовища, які з'єднуються із вхідними контактами елементів підсистеми S_μ.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 3 (29)

Вводиться однозначний оператор, що називається оператором сполучення елементів та поєднує вхідний контакт $X_i^{(j)}$ із вихідним контактом $Y_l^{(j)}$ [15]:

$$Y_l^{(k)} = R\left(X_i^{(j)}\right), \quad (1)$$

де область визначення на множині $\bigcup_{j=0}^{N}\left[X_i^{(i)}\right]_1^m$ та область значень на множині $\bigcup_{k=0}^{N}\left[Y_1^{(k)}\right]_1^r$.

У роботі розглядається приклад системи S, що містить 10 елементів, об'єднаних у підсистеми таким чином: $S_\mu = \{C_1, C_2\}$ і $S_{\mu 0} = \{C_0, C_3 - C_9\}$. Припустимо, що підсистема S_μ буде МБ системи та виконуватиме функції контролю доступу.

Метод обфускації МБ передбачає такі етапи: визначення фіктивних контактів на межі підсистеми S_μ і $S_{\mu 0}$ та побудова внутрішнього оператора сполучення елементів підсистеми S_μ.

Опишемо процес визначення фіктивних контактів.

Існує дві множини контактів елементів підсистеми S_μ: множина вихідних контактів $\left[Y_l^{(j)}\right]_\mu$ всіх елементів C_j, де $C_j \in S_\mu$, з'єднаних із вхідними контактами елементів C_k, де $C_k \notin S_\mu$; множина вхідних контактів $\left[X_i^{(j)}\right]_\mu$ усіх елементів C_j, де $C_j \in S_\mu$, що з'єднані з вихідними контактами елементів C_k, де $C_k \notin S_\mu$. Для всіх елементів цих множин необхідно визначити фіктивні контакти підсистеми S_μ.

Оператор Q'_m називається оператором нумерації фіктивних контактів та визначає значення фіктивного контакту $X_i^{(0)\mu}$ залежно від вихідного контакту $Y_l^{(j)} \in \left[Y_l^{(j)}\right]_\mu$:

$$X_i^{(0)\mu} = Q'_\mu\left(Y_l^{(j)}\right). \quad (2)$$

Оператор P'_μ називається оператором нумерації фіктивних контактів та визначає значення фіктивного контакту $Y_l^{(0)\mu}$ залежно від вхідного контакту $X_i^{(j)} \in \left[X_i^{(j)}\right]_\mu$:

$$Y_l^{(0)\mu} = P'_\mu\left(X_i^{(j)}\right)\sigma_X. \quad (3)$$

Наступним етапом є побудова зв'язків між елементами в підсистемі. Існує два типи зв'язків, що необхідно розглянути. Перший тип – це внутрішні зв'язки між вхідними та вихідними контактами елементів C_j, де $C_j \in S_\mu$. Другий тип – це зв'язки між вхідними та вихідними контактами елементів C_j підсистеми S_μ із вхідними та вихідними контактами елемента C_k, де $C_k \notin S_\mu$.

У першому випадку задано множини контактів $\left[X_i^{(j)}\right]_1^m$ і $\left[Y_l^{(j)}\right]_1^r$ для елементів C_j, де $C_j \in S_\mu$. Оператор сполучення елементів R_μ у цьому разі дорівнює R. У другому випадку в підсистемі S_μ мають бути контакти $X_i^{(0)\mu}$ та $Y_l^{(0)\mu}$, контакт $X_i^{(0)\mu}$ з'єднує вхідні контакти фіктивного елемента $C_0^{(\mu)}$ з вихідними контактами елементів підсистеми S_μ, контакт $Y_l^{(0)\mu}$ з'єднує вихідні контакти фіктивного елемента $C_0^{(\mu)}$ із вхідними контактами елементів підсистеми S_μ.

З допомогою оператора сполучення R_μ визначається схема сполучення елементів підсистеми S_μ:

$$Y_l^{(k)} = R_\mu\left(X_i^{(j)}\right). \quad (4)$$

Сполучення елементів підсистеми S_μ наведені в табл. 1.

Таблиця 1. *Сполучення елементів підсистеми* S_μ

j \ i	1	2	3	4
0	1,1	1,2	1,3	2,2
1	0,1	0,2	2,1	-,-
2	0,3	0,4	-,-	-,-

У табл. 1 елементу $C_0^{(\mu)}$ відповідає рядок 0, елементу C_1 – рядок 1, елементу C_2 – рядок 2. На перетині рядків з номерами елементів системи (j) і стовпців із номерами її вхідних контактів (i) розміщена пара чисел (k, l), що позначає номер елемента (k) і номер його вихідного контакту (l), до якого під'єднаний контакт (i). Фіктивні контакти $X_i^{(0)\mu}$ та $Y_l^{(0)\mu}$ відповідають вхідним і вихідним контактам C_0^μ відповідно. У табл. 1 подана інформація, пов'язана з під'єднанням МБ (S_μ) і основного проєкту $(S_{\mu 0})$. Ця інформація необхідна

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №3 (29) ISSN 2524-2296 (online)

для програмування підсистеми S_μ на наступних етапах проєктування.

У запропонованому способі проєктування безпечної електронної системи обов'язковий етап розроблення механізму контролю доступу додається в цикл розроблення проєкту. Завдяки обфускації приховується функціонал і структурні деталі МБ, а також забезпечуються такі властивості МБ: стає захищеним від несанкційного доступу і стає таким, щоб його неможливо було обійти.

Експериментальне оцінювання можливостей методу

Розглянемо експериментальне оцінювання потенційних переваг технології реконфігурації, що використовується для реалізації підходу обфускації МБ. Детальний опис фізичного експерименту як інструменту моделювання з метою демонстрації апаратної реалізації запропонованого методу із застосуванням платформи розроблення системи на кристалі (SoC) є достатньо специфічним і громіздким, що виводить його за межі цієї роботи. Обмежений обсяг статті не дає змогу описати докладніше експериментальне оцінювання методу. З огляду на це розглянемо основні концептуальні моменти.

У цій роботі запропонований метод обфускації проєкту електронних систем для захисту проєкту від різних форм атак. У межах технології часткової реконфігурації SoC основна концепція підходу має свої особливості, подані нижче.

Часткова реконфігурація – це можливість повторно конфігурувати обрані області FPGA в будь-який час після її початкової конфігурації. Проєкт системи на кристалі (SoC) S поділяється на дві підсистеми: S_μ, яка є МБ проєкту, і $S_{\mu 0}$, що є базовим проєктом системи S. Це означає, що проєкт загалом може бути розроблений майже повністю в ненадійному середовищі, за винятком самого *RM*, який розробляється повністю в довіреному середовищі. Ці функції дають змогу розробникам ближче інтегрувати аспект безпеки в процес проєктування системи. Інформація з табл. 1 використовується для програмування (реконфігурації SoC) підсистеми S_μ на наступних етапах і в довіреному середовищі. Практично ми приховуємо функціонал та структурні деталі МБ.

У цій статті продемонстровано підхід до обфускації МБ на основі частково реконфігурованих проєктів на FPGA. Запропонований підхід подано на архітектурі Xilinx Artix 7 FPGA сімейства ПЛІС сьомого покоління, призначеного для високопродуктивних систем. Розглянутий підхід демонструється на платі розробки Nexys 4 DDR на основі пристрою Xilinx Artix 7 XCA100T. Для проєктування використовується програмне забезпечення Xilinx Vivado.

Висновки

У статті запропоновано метод обфускації проєкту електронних систем на основі агрегації, який полягає в тому, що приховується під'єднання монітора безпеки, щоб зловмисник не міг отримати його функціональність та оригінальну структуру. Підхід для проєктування на основі обфускації передбачає, що інтегральна схема модифікується й приховуються функціональні та структурні властивості проєкту, що ускладнює для зловмисника додавання троянів.

Обфускація на основі агрегації полягає в тому, що монітор безпеки розглядається як окрема підсистема, пов'язана з основним проєктом, і таблиця з'єднання елементів підсистеми містить інформацію, пов'язану з під'єднанням монітора безпеки до основного проєкту. Отже, приховуються структурні деталі та функціонал монітора безпеки.

Часткова реконфігурація дає змогу повторно конфігурувати обрані області FPGA після її початкової конфігурації. Завдяки цьому проєкт може бути розроблений майже повністю в ненадійному середовищі, а для підсистеми, що є монітором безпеки, може бути здійснено програмування (реконфігурація SoC) на наступних етапах і в довіреному середовищі. Отже, забезпечуються властивості монітора безпеки: він має бути захищеним від несанкційного доступу та стати таким, щоб його неможливо було обійти.

Подальша робота полягає в розв'язанні таких завдань: додавання етапу створення механізму контролю доступу в цикл розроблення проєкту електронної системи; теоретичний аналіз і математичне моделювання проєкту електронної системи, який виконаний з використанням монітора безпеки, для оцінювання стійкості запропонованої схеми обфускації.

Список літератури

1. Hardware Trojan Attacks: Threat Analysis and Countermeasures / S. Bhunia et al. *Proceedings of the IEEE*. 2014. Vol. 102. P. 1229–1247. DOI: http://dx.doi.org/10.1109/JPROC.2014.2334493
2. Chakraborty R. S., Narasimhan S., Bhunia S. Hardware Trojan: Threats and emerging solutions. *IEEE International High Level Design Validation and Test Workshop*. 2009. P. 166–171. DOI: http://dx.doi.org/10.1109/HLDVT.2009.5340158
3. Li H., Liu Q., Zhang J. A survey of hardware Trojan threat and defense. *Integration*. 2016. Vol. 55. P. 426–437. DOI: https://doi.org/10.1016/j.vlsi.2016.01.004
4. Francq J. Hardware Trojans Detection Methods. *Cassidian Cybersecurity, in TRUDEVICE*. 2013. P. 36–40.
5. Saqib F., Plusquellic J. VLSI Test and Hardware Security Background for Hardware Obfuscation. *In: Forte D., Bhunia S., Tehranipoor M. Hardware Protection through Obfuscation. Springer*. 2017. DOI: https://doi.org/10.1007/978-3-319-49019-9_2
6. Development and Evaluation of Hardware Obfuscation Benchmarks / S. Amir et al. *Journal of Hardware and Systems Security*. 2018. Vol. 2. P. 142–161. DOI: https://doi.org/10.1007/s41635-018-0036-3
7. Schell R. R., Brinkley D. L. Evaluation Criteria for Trusted Systems. *In: Abrams M. D., Jajodia S., Podell H. J. Information Security: An Integrated Collection of Essays. IEEE Computer Society Press*. 1995. P. 137–159.
8. Gorbachov V., Batiaa A. K. Overview of security problems and the design of secure electronic systems. *Radiotekhnika*. 2017. Vol. 4. No. 191. P. 113–119. DOI: https://doi.org/10.30837/rt.2017.4.191.10
9. Bishop M. Computer Security: art and science. Addison-Wesley. ISBN 0-201-44099-7. 2002.
10. Anderson J. Computer Security Technology Planning Study. *Technical Report ESD-TR-73–51*. 1972.
11. Securing Computer Hardware on the Base of Reference Monitor Obfuscation / V. Gorbachov et al. *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology*. 2018. P. 406–410. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632147
12. Irvine C. E. The Reference Monitor Concept as a Unifying Principle in Computer Security Education. 1999. P. 27–37.
13. Пономаренко О. Є., Горбачов В. О. Агрегація структурної моделі складних мережних систем. *Системи управління, навігації та зв'язку. Збірник наукових праць*. 2023. Т. 1. № 71. С. 138–144. DOI: https://doi.org/10.26906/SUNZ.2023.1.138
14. Dimension Reduction for Network Systems Using Structure Model Aggregation / V. Gorbachov et al. *International Journal of Design & Nature and Ecodynamics*. 2020. Vol. 15. No. 1. P. 13–23. DOI: https://doi.org/10.18280/ijdne.150103
15. Formal transformations of structural models of complex network systems / V. Gorbachov et al. *Proceedings of the IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT'2018.* Kyiv, Ukraine. 2018. P. 473–477. DOI: https://doi.org/10.1109/DESSERT.2018.8409175

References

1. Bhunia, S., Hsiao, M. S., Banga, M., Narasimhan, S. (2014), "Hardware Trojan Attacks: Threat Analysis and Countermeasures", *Proceedings of the IEEE*, Vol. 102, P. 1229–1247. DOI: http://dx.doi.org/10.1109/JPROC.2014.2334493
2. Chakraborty, R. S., Narasimhan, S., Bhunia, S. (2009), "Hardware Trojan: Threats and emerging solutions", *IEEE International High Level Design Validation and Test Workshop*, P. 166–171. DOI: http://dx.doi.org/10.1109/HLDVT.2009.5340158
3. Li, H., Liu, Q., Zhang, J. (2016), "A survey of hardware Trojan threat and defense", *Integration*, Vol. 55, P. 426–437. DOI: https://doi.org/10.1016/j.vlsi.2016.01.004
4. Francq, J. (2013), "Hardware Trojans Detection Methods", *Cassidian Cybersecurity , in TRUDEVICE*, P. 36–40.
5. Saqib, F., Plusquellic, J. (2017), "VLSI Test and Hardware Security Background for Hardware Obfuscation", *In: Forte, D., Bhunia, S., Tehranipoor, M.* "*Hardware Protection through Obfuscation. Springer*". DOI: https://doi.org/10.1007/978-3-319-49019-9_2
6. Amir, S., Shakya, B., Xu, X., Jin, Y., Bhunia, S., Tehranipoor, M. M., Forte, D. (2018), "Development and Evaluation of Hardware Obfuscation Benchmarks", *Journal of Hardware and Systems Security*, Vol. 2, P. 142–161. DOI: https://doi.org/10.1007/s41635-018-0036-3
7. Schell, R. R., Brinkley, D. L. (1995), "Evaluation Criteria for Trusted Systems", *In: Abrams, M. D., Jajodia, S., Podell, H. J.*, "*Information Security: An Integrated Collection of Essays*", *IEEE Computer Society Press*, P. 137–159.
8. Gorbachov, V., Batiaa, A. K. (2017), "Overview of security problems and the design of secure electronic systems", *Radiotekhnika*, Vol. 4, No. 191, P. 113–119. DOI: https://doi.org/10.30837/rt.2017.4.191.10
9. Bishop, M. (2002), *Computer Security: art and science*, Addison-Wesley. ISBN 0-201-44099-7.
10. Anderson, J. (1972), "Computer Security Technology Planning Study", *Technical Report ESD-TR-73–51*.
11. Gorbachov, V., Batiaa, A. K., Ponomarenko, O., Kulak, E. (2018), "Securing Computer Hardware on the Base of Reference Monitor Obfuscation", *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology*, P. 406–410. DOI: 10.1109/INFOCOMMST.2018.8632147
12. Irvine, C. E. (1999), "The Reference Monitor Concept as a Unifying Principle in Computer Security Education", P. 27–37.
13. Ponomarenko, O., Gorbachov, V. (2023), "Aggregation of structural model of complex network systems", *Control, Navigation and Communication Systems. Academic Journal*, Vol. 1 (71), P. 138–144. DOI: https://doi.org/10.26906/SUNZ.2023.1.138

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №3 (29)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

14. Gorbachov, V., Sytnikov, D., Ryabov, O., Batiaa, A. K., Ponomarenko, O. (2020), "Dimension Reduction for Network Systems Using Structure Model Aggregation", *International Journal of Design & Nature and Ecodynamics*, Vol. 15, No. 1, P. 13–23. DOI: https://doi.org/10.18280/ijdne.150103
15. Gorbachov, V., Batiaa, A. K., Ponomarenko, O., Romanenkov, Y. (2018), "Formal transformations of stuctural models of complex network systems", *Proceedings of the IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT'2018*, Kyiv, Ukraine, P. 473–477. DOI: https://doi.org/10.1109/DESSERT.2018.8409175

Надійшла (Received) 01.09.2024

Відомості про авторів / About the Authors

Пономаренко Ольга Євгеніївна – Харківський національний університет радіоелектроніки, аспірант кафедри електронних обчислювальних машин, Харків, Україна; e-mail: olha.ponomarenko@nure.ua; ORCID ID: https://orcid.org/0009-0002-4634-6552

Горбачов Валерій Олександрович – кандидат технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри електронних обчислювальних машин, Харків, Україна; e-mail: valeriy.gorbachov@nure.ua; ORCID ID: https://orcid.org/0000-0003-3423-2371

Ponomarenko Olha – Kharkiv National University of Radio Electronics, Postgraduate Student at the Department of Electronic Computers, Kharkiv, Ukraine.

Gorbachov Valeriy – PhD (Engineering Sciences), Professor, Kharkiv National University of Radio Electronics, Professor at the Department of Electronic Computers, Kharkiv, Ukraine.

AGGREGATION-BASED OBFUSCATION METHOD FOR ELECTRONIC SYSTEMS DESIGN

Hardware Trojan attacks relate to malicious modifications of integrated circuits during design or manufacturing, involving untrusted design tools or components. Such modifications can lead to undesired behavior of integrated circuits or the appearance of hidden data leakage channels. There are various methods of classification, detection and prevention of hardware Trojans insertion. One approach to prevent of Trojans insertion is an obfuscation-based design approach. This approach is based on hiding the functional and structural properties of the design, which makes it difficult for an attacker to insert Trojans. **The subject matter of research** is an aggregation-based obfuscation method for electronic systems design. **The goal of the work** is to study the process of aggregation-based obfuscation of the electronic systems design. The main idea is that the development and connection phase of the reference monitor is performed in a trusted environment. Thus, an attacker will not be able to obtain its functionality and original structure. **The relevance of the work** lies in the fact that this approach prevents the possibility of functioning of hardware Trojans. **The following tasks were solved in the work**: development and study of an aggregation-based obfuscation algorithm for electronic systems design; implementation of the reference monitor presentation as a separate subsystem associated with the main design; experimental evaluation of the possibilities of the method. **As a result of the work** the aggregation-based obfuscation method for electronic systems design was demonstrated; reference monitor was presented as a separate subsystem associated with the main design; experimental evaluation of the possibilities of the method was demonstrated. The studies allow us to **conclude**: the obfuscation-based design approach is that the integrated circuit is modified, thus, the functional and structural properties of the design are hidden, which makes it difficult for an attacker to insert Trojans. Aggregation-based obfuscation considers the reference monitor as a separate subsystem associated with the main design.

Keywords: hardware security; obfuscation of electronic systems design; reference monitor; aggregation.

Бібліографічні описи / Bibliographic descriptions

Пономаренко О. Є., Горбачов В. О. Метод обфускації проєкту електронних систем на основі агрегації. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 3 (29). С. 57–63. DOI: https://doi.org/10.30837/2522-9818.2024.3.057

Ponomarenko, O., Gorbachov, V. (2024), "Aggregation-based obfuscation method for electronic systems design", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (29), P. 57–63. DOI: https://doi.org/10.30837/2522-9818.2024.3.057