к.т.н. Застело Г.І. (ВІТІ)
к.т.н. Кулініч О.М. (ВІТІ)
к.т.н. Липський О.А. (ІСЗЗІ НТУУ КПІ)

СПОСОБИ ВИЯВЛЕННЯ ВБУДОВАНИХ ЗАКЛАДНИХ ВУЗЛІВ У СПЕЦІАЛІЗОВАНИХ ІНТЕГРАЛЬНИХ СХЕМАХ

Розглядаються проблемні питання виявлення встановлених закладних пристроїв у вигляді апаратного модуля, що інтегрується в окрему спеціалізовану інтегральну мікросхему – основу елементній базі, що використовується для побудови спеціалізованих інформаційних систем.

Застело Г. И., Кулинич О. Н., Липский А. А. Способы обнаружения закладных узлов, встроенных в специализированные интегральные схемы. *Рассматриваются проблемные вопросы обнаружения установленных закладных устройств в виде аппаратного модуля, которые интегрируется в отдельную специализированную интегральную микросхему – основу элементной базы, используемой для создания специализированных информационных систем.*

G. Zastelo, O. Kulinich, A. Lipski Some techniques of exposure of the tabs built in the specialized integral systems. *The issues of exposure of the module tabs are examined, that are integrated into a separate specialized integral microcircuit – a basis of the element base that is used for the construction of the specialized information systems.*

Ключові слова: *закладні пристрої, апаратний троян, спеціалізована інтегральна мікросхема.*

Постановка завдання. Аналіз сучасних засобів спеціального призначення та систем керування показує, що їх розвиток здійснюється шляхом зменшення лінійних розмірів при одночасному збільшені обчислювальної потужності та розширені функціональних можливостей за рахунок використання спеціалізованих інтегральних схем (ASIC – Application – Specific Integrated Circuit). Це у свою чергу може призвести до несанкціонованого доступу та встановлення апаратних закладних пристроїв. Поняття фізичної безпеки включає протидію зовнішньому втручанню та здатність виявити таке втручання, якщо воно відбулося. Одним з елементів фізичної безпеки є компонування мікросхеми, що здійснює обробку інформації. Це компонування забезпечує як захищеність від деяких видів зовнішнього втручання, так і здатність таке втручання виявити [1].

Ми давно звикли до того, що практично будь-яке програмне забезпечення може бути заражене – і, за визначенням, не гарантує повній безпеці. Проте тепер уже рисують сценарій нової небезпеки. Тоді як в процесор інтегрується все більше корисних функцій, постійною частиною обчислювальної системи може стати дистанційно керований троян. Це попередження не можна вважати безпідставним хоч би тому, що у світі все частіше з'являються флеш-накопичувачі з інтерфейсом USB, що заражаються шкідливими програмами вже у момент виробництва.

У вересні 2007 року Ізраїль атакував підозрілий ядерний об'єкт, розташований на території Сирії. Незадовго до початку нальоту ізраїльської авіації суперсучасні радари сирійської армії, які використовувалися в системі ППО, вийшли з ладу. Після цього випадку експерти по комп'ютерній безпеці забили на сполох: на їх думку, причиною такої несподіваної відмови техніки став „бэкдор", закладений в чіпи радарів ще на етапі виробництва. У військових відомствах різних країн до подібної можливості відносяться дуже серйозно і побоюються, що існуючі системи озброєнь вже заражені і одного прекрасного дня можуть дистанційно деактивувати. Заради гарантій, щонайменше, на майбутнє, все частіше висувається вимога, щоб постачальники комп'ютерних систем надавали точні дані компаній, що беруть участь в розробці процесорів, і їх персоналу того, що має відповідний допуск [2].

Представлена проблема стає насущною раз фахівці вважають, що в обороті вже є заражені процесорні чіпи, які тільки і чекають команди на активацію. У простому випадку вони можуть заблокувати функціональні можливості ПК або мобільних телефонів. Проте найвірогідніший, сценарій – це непомітне шпигунство на системному рівні, наприклад, відправка копій електронних листів або даних на деякі секретні сервери. Тому ***метою***

статті є аналіз варіантів встановлення апаратних закладних пристроїв та підходів щодо виявлення цього факту.

Аналіз останніх публікацій. Основи створення спеціалізованих інтегральних мікросхем та особливості розробці їх дизайну викладені у [3].

Передбачається наявність декількох шляхів, що дозволяють здійснити несанкціоновану модифікацію структурних елементів чипу, реалізував тим самим апаратну закладку [4].

Кроки, які запропоновані фахівцями з метою посилення вбудованих контролюючих функції чипу, наведені у [5]. Однак питання пошуку можливих методів виявлення апаратних троянів з урахуванням результатів аналізу варіантів встановлення апаратних закладних пристроїв потребують додаткового опрацювання.

Виклад основного матеріалу. Сучасна ситуація в області розробки напівпровідникових мікросхем, що склалася у світі така, що в розробці дизайну одного чіпа сьогодні зайняті сотні підприємств, розкиданих по усій планеті. Всього у світі існує близько 1550 таких фірм, кожна з яких спеціалізується на певних функціональних блоках для процесорів. Ці компанії щорічно розробляють тисячі CPU [6].

Основою створення спеціалізованих інтегральних схем є модулі інтелектуальної власності IP (Intellectual Properties), що розповсюджуються у вигляді програмних модулів описаних на мові HDL (Hardware Distribution Language). Особливістю ASIC (Application - Specific Integrated Circuit) є висока швидкодія, малий рівень чутливості до зовнішніх факторів та мала ціна при великих об’ємах виробництва. Більшість світових виробників напівпровідникової продукції при створенні ASIC корпусів на своїх технологічних лініях використовують надійні і перевірені часом архітектурні рішення відомих виробників таких як: PowerPC, ARM, MIPS, SPARC та ін. Особливістю останніх ASIC є можливість встановлення повноцінної операційної системи на базі Open Source та наявність декількох обчислювальних процесорних модулів [7].

Отже, небезпечною є тенденція, коли закладні пристрої входять до складу вбудованої системи у вигляді програмного або апаратного модуля, що інтегрується в окрему спеціалізовану інтегральну мікросхему ASIC. Нажаль, на даний годину відсутні надійні та перевірені методи щодо пошуку закладних пристроїв на апаратному та програмному рівні, а це робить спеціалістів із захисту інформації беззахисними перед даними видами загроз. Таким чином, на підставі вище зазначеного існує актуальне завдання щодо розробки нових методів пошуку закладних пристроїв у елементній базі, що використовується для побудови засобів захисту інформації. Пошук закладних пристроїв на апаратному рівні ASIC, зазвичай реалізується за рахунок руйнування захисного кулі мікросхеми із подальшим фотографуванням та дослідженням. Цей метод є дуже складний і потребує великих капіталовкладень, а враховуючи, ті що більшість мережевого і комунікаційного обладнання виготовляється на спеціалізованих мікросхемах, то процес дослідження обладнання на наявність закладних пристроїв може тривати до безкінечності. Дослідження вбудованих систем на програмному рівні вимагає наявності вільного доступу до програмного забезпечення дослідного зразка, встановлення на ньому програмного дезасемблера та засобів відлагодження, що не завжди можливо. Таким чином, при нинішніх методах розробки чіпів існує чисто статистична вірогідність неконтрольованого дизайну

Залежно від характеристик апаратні трояни (АТ) діляться на декілька груп (рис. 1). Деякі лише крадуть особисті дані, інші здатні нанести серйозний ущерб об’єктам інфраструктури, знищивши їх процесори в самий непідходящий момент.

Сьогоднішня схема дизайну процесорів зазвичай виглядає так: фірма-замовник, що здійснює загальне виробництво, інтегрує у свій продукт окремі блоки, що розробляються численними суміжними підприємствами. Саме тут бачиться головне вразливе місце. Якщо хтось захоче впровадити в чіп троян, він може здійснити свій злий намір фактично на будь-якій стадії розробки і виробництва – від побудови логічної схеми до виготовлення на заводі.

Рис. 1 Класифікація апаратних троянів

При сучасній складності окремих блоків жодне підприємство не в змозі перевірити усі теоретично можливі сценарії їх використання, тому зазвичай тестують лише основні функціональні можливості, а також типові варіанти помилок. Проте ніхто не знає, як реагуватиме той або інший блок, якщо він отримає деякий незапланований вхідний сигнал.

Якщо впровадитися у виробничу фірму не вдалося, то завжди залишається можливість модифікації вже готових чіпів. Правда, для цього знадобиться дуже дороге устаткування – оператор установки для того, що іонного, що труїть за допомогою сфокусованого пучка іонів змінює зв'язки між окремими логічними елементами чіпа. Якщо ця мікросхема широко використовується в об'єктах інфраструктури, атомних станціях і навіть системах озброєння, то наслідки подібної атаки можуть мати найруйнівніші наслідки. Крім того, потенційним хакерам вигідно заражати чіпи серверів або комп'ютерів приватних підприємств, адже такі дії можуть принести великі гроші. Протестувати мікросхему на наявність в ній усіх незадокументованих розробником функцій неможливо зважаючи на високу складність сучасних кремнієвих чіпів. Адже навіть на етапі перевірки специфічних функцій систем на чіпі, в які, окрім обчислювальних ядер, вбудовані різні контролери, пам'ять і інші елементи, практично неможливо досліджувати усі 100 % площі поверхні процесора.

Для оцінки ймовірності отримання інформації, що знаходиться в середині обчислювального модуля співпроцесорів може використовується критерій переваг це зумовлено тим, що статистична інформація, щодо методів і спроб несанкціонованого отримання інформації із обчислювальних процесорів і мікроконтролерів не завжди є правдивою. В цьому випадку передбачається, що ймовірність реалізації загрози визначається наступними факторами:

– привабливістю активу (цей показник використовується при розгляді загроз навмисного впливу з боку людини);

– можливістю використання активу для одержання доходу (цей показник використовується при розгляді загроз навмисного впливу з боку людини);

– технічними можливостями реалізації загрози з боку зловмисника при здійснені атаки;

– ступенем легкості, з яким може бути використана та чи інша атака.

Універсальним критерієм ефективності є критерій „затрати – ефективність". Згідно з цим критерієм, найбільш привабливим є такий варіант, в якому при найменших витратах забезпечується найбільша ефективність. З урахуванням того, що у вартісному виразі ефект дій зловмисника визначається величиною збитку, пов'язаного з реалізацією інформаційної загрози, вираз для оцінки ймовірності P_j реалізації j–ї загрози інформації з використанням критерію переваги можна записати у виді:

$$P_j = \frac{Q_j}{C_j \sum_{i=1}^{n} \frac{Q_i}{C_i}} = \frac{Q_j}{C_j \sum_{\substack{i=1 \\ i \neq j}}^{n} \frac{Q_i}{C_i} + Q_j}, \quad (1)$$

де j – номер загрози інформації; n – кількість розглянутих у ході аналізу ризиків способів реалізації загроз інформації; Q_i – оцінка збитку, пов'язаного з використанням i – го способу реалізації загрози; C_i – оцінка витрат порушника по підготовці і реалізації загрози в i – й спосіб.

Способи виявлення апаратних троянів діляться на дві групи:

– передвиробничі;

– поствиробничі.

У першому випадку завданням інженерів є знаходження підозрілих блоків в логічній структурі чіпа, які могли з'явитися в нім з вини недобросовісних співробітників або сторонніх компаній, залучених до розробки мікросхеми. Виявити впроваджені на етапі виробництва трояни можна також методами другої групи.

Одним з поствиробничих способів виявлення АТ є метод деструктивного тестування. Його суть полягає в послідовному видаленні і фотографуванні кожного з шарів чіпа (у сучасних процесорах може бути більше десяти шарів) і подальшому порівнянні отриманих фотографій з початковою маскою процесора, по якій він виготовлявся на фабриці.

Для відтворення компонування модулів можна використовувати оптичний мікроскоп, оснащень CCD – камерою. Основні модулі мікросхеми (ROM, EEPROM, RAM, процесор, шини) добрі видно на фотознімку, отриманих за допомогою CCD – камери із високою роздільною здатністю. Для отримання глибших шарів мікросхем, застосовують фізичне травлення із подальшою обробкою на основі розпізнання образів та створенням тривимірної моделі чіпа. Інший спосіб обстеження кристалу мікросхеми отримав назву ручного зондування. Він заснований на використанні оптичного мікроскопа і зонду, в якості зонду використовується тонка вольфрамова голка, яка з'єднується із шинами кристалу без їх руйнування. Зонд оснащень підсилювачем і підключається до спеціального цифрового процесора обробки сигналів, який записує сигнали отримані від процесора, а також забезпечує напругу, встановлення сигналів Reset, тактовий сигнал (Clock) та інші вхідні сигнали, необхідні для функціонування мікросхеми в активному режимі.

Для реалізації ручного і променевого способу зондування окрім виконання процедури витягання кристалу мікросхеми необхідно зруйнувати деяку частини пасивації. Шар пасивації захищає мікросхему від деяких видів опромінювання і шкідливих дій навколишнього середовища. Для видалення кулі пасивації використовують ультрафіолетове випромінювання або „зелені" лазери, які руйнують куля пасивації. Іноді для руйнування невеликої за розмірами ділянки пасивації використовують свердлення.

Хоча ця тактика з високою мірою вірогідності дозволяє виявити зайві транзистори і доріжки, вона дуже трудомістка. Крім того, перевірити усю партію мікросхем деструктивним методом неможливо, оскільки в його процесі чіп повністю руйнується. Альтернатива деструктивному тестуванню – це метод сканування мікросхеми рентгенівськими променями, який дозволяє добитися аналогічного ефекту без руйнування кристала. Існує також променевий спосіб зондування чіпа, при якому використовується сфокусований промінь іонів галію (Focused Ion Beams або FIB). Іони галію прискорюються і фокусуються у вакуумній камері в промінь діаметром 5 – 10 нанометрів. Він випромінюється рідким катодом із напругою 30 кіловольт, іони галію мають струм від 10 – 12 до 10 – 8 ампер. Сфокусований промінь іонів галію може відтворити компонування мікросхеми завдяки фіксації вторинного випромінювання. Роздільна здатність складає до 5 нанометрів.

Іншим різновидом променевого способу зондування кристалу мікросхеми є використання електронних променів. Для розгону електронів застосовується електрична напруга близько 2,5 кіловольт, у результаті створюється струм силою близько 5 наноампер. При цьому кількість і енергія вторинних електронів з'являються індикаторами електричного полю на поверхні кристалу і дозволяє робити обстеження сигнальних ліній із роздільною здатністю у долі мікрона. Останнім часом з'явився ще один різновид променевого способу обстеження кристалу мікросхеми із застосуванням інфрачервоного лазера. Використовується

така частота опромінювання кристалу, при якій її кремнієва основа стає прозорою для лазерного променю. При цьому виконується виміри струмів, що відображають логічний стан окремих транзисторів. Також практикується спосіб порівняння результатів роботи випробовуваної мікросхеми з тими, що видає так званий „золотий" чіп (ідеальний зразок), трояни в якому свідомо відсутні. Існують і менш витратні методики – наприклад, фаззинг (fuzz testing). Зважаючи на те що сучасні мікросхеми мають дуже складну структуру, їх розробники частенько користуються стандартними блоками, серед яких, – відладчик JTAG. Він потрібний для того, щоб прочитувати налагоджувальну інформацію з „ніг" чіпа, не вставляючи його в роз'єм. Шляхом посилки нестандартних запитів можна вичислити деякі створені або змінені із злим наміром блоки тестуємої мікросхеми.

Подібні підходи допомогли співробітникам відділу безпеки в комп'ютерній лабораторії Кембріджського університету, вичислити „бэкдор" в китайському чіпі. Після сканування за методикою, розробленою ученими університету, в мікросхемі була виявлена небезпечна уразливість, яка дозволяла відключати криптографічний захист, міняти ключ шифрування AES, діставати доступ до незашифрованого потоку даних або навіть зовсім вивести чіп з ладу. Дослідникам вдалося витягнути секретний ключ, який активував „бэкдор".

На думку фахівців, для захисту від апаратних троянів, необхідно реалізувати в чіпі шість функцій:

1. **Контроль пам'яті.** Кожному блоку чіпа призначається одна, строго певна робоча область пам'яті. Будь-яка спроба звернутися до іншої області відхиляється.
2. **Контроль шини** запобігає блокуванню шини мікросхеми з боку зараженого блоку. Це дозволить зберегти функціональні можливості усієї системи в цілому.
3. **Моніторинг введення/виводу** уберігає від крадіжки даних, задаючи кожному блоку певну поведінку для операцій введення/виводу і не допускаючи ніяких відхилень.
4. **Самотестування функціональних блоків**. Чіп самостійно проводить регулярну перевірку окремих блоків, з яких він складається, на предмет правильності їх поведінки. При будь-яких аномаліях блок закривається.
5. **Самопрограмуючаяся апаратна логіка**, забезпечує заміну функціонального мінімуму зараженого і замкнутого блоку, щоб відключення інфікованих частин процесора не привело до відмови усієї системи.
6. **Попередження у разі атаки**. Блок, що піддався атаці, посилає попередження іншим блокам, а вони реагують строго певним чином – відправляють пошкоджений блок в карантин.

Додаткове обчислювальне навантаження, необхідне для реалізації в процесорі шести запропонованих їм функцій, що підвищують безпеку, не представляє для актуальних чіпів серйозної проблеми. Група американських і європейських дослідників опублікувала наукову роботові, в якій описала новий потайний метод впровадження троянів в мікросхему таким чином, щоб ці зміни не можна було виявити за допомогою мікроскопа або функціональних тестів. Метод полягає в тому, щоб змінювати полярність допанта на певних ділянках транзистора (рис. 2). У мікросхемах процесора допант виконує завдання з підвищення питомої електричної провідності. У процесі виробництва теоретичний можна змінити властивості транзистора потрібним зловмисникові чином та отримати контроль над цільовим пристроєм [8]. У роботі представлено два приклади того, як подібну атаку можна провести на практиці. У одному з

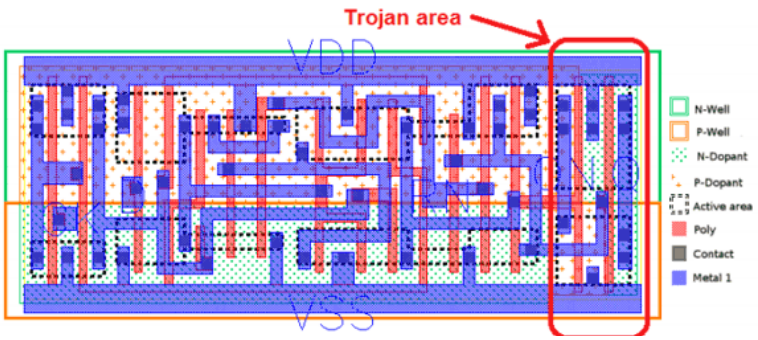

Рис. 2 Приклад вбудові апаратного трояна в мікросхему.

цих прикладів наводитися модифікація модуля ГПВЧ в процесорах Intel Ivy Bridge. У цьому процесорі генеруються 128 – бітові псевдовипадкові числа, ГПВЧ в ньому складається з двох частин – джерело ентропії і система цифрової пост-обробки. Один з модулів пост-обробки видає результат на основі невідомих 128 – бітних випадкових чисел від джерела ентропії і невідомих 128 – бітних чисел, обчислюваних в процесі обробки, використовуючи алгоритм шифрування AES. Якщо зловмиснику вдасться змінити певна кількість з 128 регістрів на постійні значення, то вірогідність вгадування згенерованого блоком ГПВЧ числа (тобто і злому шифру) зросте з $1/2^{128}$ до $1/2^{m}$, де m – кількість залишених без зміни регістрів. Виявити збій в роботі блоку ГПВЧ модифікованого процесора навіть при m = 32 буде практично неможливо, адже він успішно пройде усі тести.

Підсумуємо, що уразливості можуть бути впроваджені в мікросхему як на етапі проектування, так і виробництва. Відшукати декілька тисяч шкідливих транзисторів серед мільйонів корисних непросто. Тому великі концерни, CPU, що виробляють, повинні змінити дизайн своїх продуктів – чіпи повинні мати вбудований компонент, що відповідає за безпеку.

Висновки. Таким чином, замість того, щоб впроваджувати в мікросхему додаткові напівпровідникові елементи, для виготовлення апаратного трояна досить вибірково змінити полярність допанта (змінити роботу наявних в чіпі транзисторів) і тим самим вплинути на роботу криптографічного блоку процесора потрібним чином. Створені за цією методикою апаратні закладки неможливо виявити більшістю методів, включаючи скануючу мікроскопію і порівняння з еталонними чіпами. Для вирішення завдання щодо захисту від закладних пристроїв можуть слугувати власні розробки, що відбуваються із поетапним їх дослідженням, розробкою відповідних технічних умів та математичних моделей, вибором елементної бази, програмного забезпечення, виготовленням готової продукції, а при вдалій реалізації зазначених етапів – закупівля IP модулів для реалізації вітчизняних ASIC. Це дозволити створити власну лінійку обладнання із повним технологічним циклом, починаючи від розробки із закінчуючи етапом утилізації, що забезпечить більш високий рівень захисту від апаратних закладних пристроїв. Напрямом подальших досліджень є аналіз наявних методів виявлення допантів, які основані на дослідженнях у галузі неорганічного металоведення та нанотехнологій.

ЛІТЕРАТУРА

1. „Як створюються і чим небезпечні віруси для мікросхем” [Електронний ресурс]. – Режим доступу: http://mediatek-club.ru/virusy-dlya-mikroshem-kak-sozdayutsya-i-oni-chem-opasny.

2. Голдовский И. Банковские микропроцессорные карты / И. М. Голдовский – М.: ЦИПСиР: Альпина Паблишерз, 2010. – 686 с.

3. Уилкинсон. Основи проектування цифрових схем.: Пер. з англ. / Уилкинсон, Барри. – М.: „Вільямс”, 2004. – 320 с.

4. L.Lin Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering. In Cryptographic Hardware and Embedded Systems / L. Lin M. Kasper, T. Gu¨neysu, C. Paar, and W. Burleson. – CHES 2009, LNCS, pages 382–395. Springer, 2009.

5. Тимошенко А.О. Методи аналізу та проектування систем захисту інформації: курс лекцій / А.О. Тимошенко. – К.: НТУУ „КПІ”, 2007. – 176 с.

6. В.Егоров. Многоядерные интегрированные сетевые процессоры высокой пропускной способности. / В. Егоров. // Электронные компоненты. – № 7 – 2009. – С. 29 – 33. curity.

7. ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT se.

8. J. Li and At-speed delay characterization for IC authentication and Trojan horse detection. In IEEE International Workshop on Hardware-Oriented Security and Trust / J. Li and J. Lach. (HOST 2008), pages 8 – 14. – 2008.