УДК 004.032.2

Ю. З. Шологон
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ВРАЗЛИВОСТІ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРФІЗИЧНИХ СИСТЕМ

Розглянуто способи захисту кіберфізичних систем. Виокремлено основні завдання, пов’язані з апаратним захистом кіберфізичних систем. Проаналізовано етапи роботи кіберфізичних систем, під час яких система є найвразливішою.

Ключові слова: кіберфізичні системи, апаратна безпека, 3PIP ядра, кібератаки.

CYBER-PHYSICAL SYSTEMS HARDWARE SECURITY VULNEABILITIES

The main methods of protecting cyber physical systems are described in this paper. The most important hardware security tasks were noticed. Analyzed staged of cyber physical systems on which systems is the most vulnerable.

Key words: cyber-physical systems, hardware security, 3PIP cores, cyber-attacks

Вступ

Швидкий розвиток сучасних технологій проектування і засобів автоматизації в останні два десятиліття привели до революції в інформаційних технологіях (ІТ). Надзвичайно швидкі персональні комп'ютери і портативні стільникові телефони, численні програми й інструменти, високошвидкісний Інтернет у всьому світі й комп'ютерні мережі змінили спосіб нашого життя. Більшість обчислювальних пристроїв є вбудованими у сучасних електронних пристроях загального користування. Вбудовані системи – це обчислювальні платформи спеціального призначення, спроектовані для виконання певних функцій управління відповідно до набору команд. Багато вбудованих системи розгорнуті у фізичних системах. Є проблема взаємодії між кіберсистемою і фізичним світом, а також забезпечення захисту даних під час цієї взаємодії

Способи апаратного захисту істотно відрізняються від програмних чи мережевих. Зазвичай апаратне проектування і виробництво відбувається перед або разом із розробленням програмного забезпечення, як результат, необхідно подбати про апаратну безпеку на ранніх стадіях розроблення продукту. У випадку зламу зловмисником апаратних засобів механізми безпеки програмного забезпечення можуть виявитися марними.

Огляд літератури

Про захист апаратного забезпечення потрібно думати навіть після закінчення його використання, тому що завжди існує ризик крадіжки даних або програмного забезпечення, яке міститься у апаратних засобах [1, 3, 7]. Саме тому потрібно дбати про безпеку апаратних засобів, починаючи від їх проектування до утилізації.

Вбудовані компоненти широко використовуються у кіберфізичних системах для координації різних обчислювальних процесів [6]. Розроблено багато підходів безпеки [2, 5], щоб запобігти проникненню шкідливих програм. КФС використовують численні гетерогенні компоненти [4, 8],

які можуть розглядатися як підсистеми, що містять прості сенсори, дротові та бездротові комунікаційні та мережеві пристрої, а також вбудовані обчислювальні системи [7]. Як наслідок, численні атаки на КФС показали [10], що безпека апаратної частини [9] є одним із основних завдань [11, 12]. У проаналізованих роботах не наведено основних задач, пов'язаних з апаратним захистом кіберфізичних систем.

Мета роботи

Метою роботи є визначення основних завдань і методів боротьби, пов'язаних із апаратним захистом кіберфізичних систем.

Означення КФС

Термін "кіберфізична система" (КФС), що запропонував Національний науковий фонд (National Science Foundation, NSF), означає інтеграцію обчислень у фізичному процесі [2]. Як правило, КФС складається з фізичного процесу, що контролюється і управляється кіберсистемою. У КФС вбудовані системи контролюються та управляються фізичним процесом, як правило, за допомогою зворотного зв'язку, фізичний процес впливає на обчислення і навпаки. КФС характеризуються великими розмірами системи, неоднорідністю ресурсів, невизначеністю динаміки системи і великою кількістю фізичних взаємодій. На відміну від традиційних вбудованих систем, спрямованих на оптимізацію обчислень у середовищі з обмеженими ресурсами, КФС спрямовані на взаємодію обчислень із фізичним середовищем.

КФС – це революція у обчислювальних системах, тому Національний науковий фонд США надає високі пріоритети дослідженням у цій галузі. КФС сьогодні можна знайти у таких галузях, як аерокосмічна, автомобільна промисловість, хімічні процеси, цивільна інфраструктура, енергетика, охорона здоров'я, транспорт та розваги. На рис. 1 зображено основні галузі застосування кіберфізичних систем.

Рис. 1. Основні галузі застосування кіберфізичних систем

Дослідження КФС охоплює нові розробки у галузях комп'ютерної архітектури, програмного забезпечення, комп'ютерних систем, мереж та інших інженерних галузей. Ця область відкриває нові можливості та створює додаткові задачі, такі як [5]:

1. Забезпечення взаємодії між розподіленими кіберфізичними системами.
2. Забезпечення надійності та захисту інформації.
3. Забезпечення контролю над гібридними ситемами.
4. Розроблення архітектури.

Традиційні вбудовані системи потребують більше гарантій безпеки, ніж платформи загального призначення. В умовах переходу до кіберфізичних систем вимоги безпеки повинні бути збільшені, щоб протистояти зростанню кількості загроз, спрямованих на пошкодження фізичних систем через кібератаки. Без підвищення безпеки КФС не можуть застосовуватись у таких галузях, як охорона здоров'я, та у інших системах, вимогливих до безпеки.

Архітектура КФС

Як правило, кіберфізичні системи побудовані у вигляді системи управління зі зворотним зв'язком. Рис. 2 ілюструє основну архітектуру КФС, у якій сенсори, виконавчі елементи (ВК) і контролери утворюють мережу елементів [7].

Рис. 2. Архітектура кіберфізичної системи

Вбудовані контролери – це обчислювальні системи, що містять набір компонентів, таких як процесори, пам'ять, пристрої введення/виведення. Ця інфраструктура розподіляється у абстрактних рівнях системи. Абстрактні рівні системи – це апаратні засоби, операційна система (ОС), програмне забезпечення і дані. Сучасні компоненти характеризуються складністю функцій і взаємодій з даними, що проходять через різні рівні системи.

Для підвищення продуктивності розроблення і зменшення витрат на дизайн вбудовані контролери часто зібрані з готових комерційних компонентів і сторонніх модулів інтелектуальної власності. Навіть вбудовані комп'ютерні системи часто застосовують програмні засоби сторонніх виробників [6]. Розробки з відкритим вихідним кодом є основним постачальником вбудованого програмного забезпечення. IP ядра широко використовуються у спеціалізованих інтегральних схемах (ASIC) і програмованих логічних матрицях (FPGA).

Готові комерційні компоненти та інтегральні схеми є уразливими для злому і зміни протягом всього процесу проектування та виготовлення. Як правило, такі компоненти не можуть бути надійними через загрозу програм-шпигунів, що можуть міститись у цих компонентах. Програми-шпигуни можуть бути вбудовані як в апаратне, так і у програмне забезпечення. Оскільки вбудовані контролери є програмованими, багато програм-шпигунів можуть туди потрапити разом із програмним забезпеченням. Саме тому захист апаратного забезпечення відіграє важливу роль.

Огляд КФС

Для того, щоб зрозуміти вимоги до безпеки кіберфізичних систем, необхідно описати їх характеристики і основні відмінності від традиційних вбудованих комп’ютерних систем та комп’ютерів загального використання. Незалежно від середовища КФС мають такі властивості [6].

1. Інтенсивна взаємодія з фізичними системами.

2. Наявність у кожному фізичному чи мережевому компоненті: програмне забезпечення міститься у всіх вбудованих системах або фізичних компонентах.

3. Взаємодія з різними мережами: у мережі КФС входять дротові та бездротові мережі (Wi-Fi, Bluetooth).

4. Взаємодія з різноманітними ресурсами з різноманітними властивостями.

5. Динамічна реорганізація / реконфігурація: КФС є дуже складними системами, тому повинні мати адаптивні можливості.

Взаємодія з фізичним світом визначає поведінку КФС, зазвичай налаштованих як системи управління зі зворотним зв'язком, у яких невелика зміна у поведінці фізичної системи зумовлює еквівалентну зміну в поведінці кіберсистеми і навпаки. Взаємодія з фізичними системами неперервна у часі й відбувається у режимі реального часу. Крім того, фізичний світ є не зовсім передбачуваним і, отже, КФС повинні бути стійкими до несподіваних змін і збоїв підсистеми. Взаємодія з фізичним світом є фундаментальною відмінністю КФС від обчислювальних платформ загального призначення, оскільки тільки користувачі можуть виконувати основні системні зміни. З погляду безпеки, оскільки взаємодія між кібер- і фізичними системами збільшується, фізичний світ стає вразливішим до атак, що виникають у кіберсистемах. Ці проблеми безпеки зумовлюють необхідність гарантування безпечного і надійного функціонування КФС.

Розмаїття компонентів відрізняє КФС від традиційних вбудованих систем, які можна розглядати як підсистеми у великих КФС. Незважаючи на велику кількість компонентів у КФС, всі вони об’єднуються для єдиного обслуговування фізичних систем. З іншого боку, КФС характеризуються не тільки різноманітністю компонентів і взаємодій, але й різноманітністю цілей і завдань. Ця різноманітність ресурсів, взаємодій і багатозадачність робить реалізацію КФС дуже складною. КФС – система з жорсткими зв'язками між обчислювальною технікою і фізичними компонентами. Зв'язки між різними підсистемами можуть бути фізично розділені й розподілені на великих відстанях. Це досягається за рахунок мережевих взаємодій у різних мережевих доменах. Це також відрізняє КФС системи від традиційних вбудованих систем, що зазвичай зосереджені на одній платформі.

У таблиці наведено порівняння властивостей КФС, вбудованих комп’ютерних систем та персональних комп’ютерів [9].

Порівняння властивостей КФС, вбудованих комп’ютерних систем та персональних комп’ютерів

	ПК	Вбудовані КС	КФС
Взаємодія з фізичним світом	Ні	Так	Так
Різноманітність компонентів	Так	Ні	Так
Різноманітність цілей	Так	Ні	Ні
Мережева взаємодія	Так	Обмежено	Так

Складнощі гарантування апаратної безпеки КФС

В останні кілька років комп'ютерна безпека привертає значну увагу з боку наукового співтовариства. Розроблені різні протоколи безпеки і стандарти, такі як IPSec, SSL, WEP і WLTS. Хоча ці протоколи безпеки теоретично можуть захистити приватне життя і конфіденційність даних, вони не можуть гарантувати апаратну безпеку засобу. Тому збільшується кількість успішних атак на апаратні засоби. Недоліком засобів апаратного захисту є те, що вони впливають на швидкодію, енергозатрати, вартість пристрою, однак порівняно з можливими ризиками ці складнощі не здаються такими суттєвими [10].

Кіберфізичні атаки використовують вразливості конкретної реалізації системи і спрямовані на злам криптографічних алгоритмів та протоколів. Вразливості КФС можуть бути спричинені ненавмисними або спеціальними змінами у роботі системи, що може призвести до втрати конфіденційності, цілісності та доступності. Загалом можна виділити три режими роботи, у яких система є найвразливішою:

1. ***Моніторинг***. Моніторинг фізичних процесів є однією з основних функцій КФС. Під час моніторингу використовуються безліч давачів для безперервного збору інформації про фізичну систему, яка потім відправляється до керуючих елементів кіберсистеми. Давач – це перетворювач,

що вимірює певні параметри фізичної системи, такі як швидкість, температура, тиск, і перетворює їх на електричні сигнали. Системи зворотного зв'язку в основному покладаються на інформацію з давачів фізичних процесів. Помилки давачів типові для всіх фізичних систем. Для захисту КФС у цьому режимі роботи було розроблено багато методів і алгоритмів, однак доволі багато кібератак сьогодні спрямовані на одержання або фальсифікування інформації, що передається давачами.

2. ***Передача інформації через мережу***. Переважно кіберфізичні системи складаються з декількох давачів і вбудованих контролерів, що взаємодіють один з одним. Мережі часто використовуються для обміну інформацією у реальному часі. Обмін інформацією між різними елементами КФС є вразливим до різних комп'ютерних загроз, таких як прослуховування, DOS атаки, модифікація даних і багато інших. Відомі методи і рішення пов'язані з підсиленням безпеки каналів зв'язку у традиційних комп'ютерних мережах. Шифрування, аутентифікація і авторизація є основними методами для забезпечення надійного передавання інформації через мережу.

3. ***Опрацювання інформації.*** На цьому етапі вбудовані керуючі пристрої опрацьовують інформацію, одержану від давачів, після чого відправляють зворотний відгук до системи. Вбудований контролер – це обчислювальна платформа, що поєднує програме й апаратне забезпечення, зберігальні елементи, пристрої вводу/виводу та пристрої зв'язку. Пристрої обробки інформації містять в собі прості мікроконтролери, одно- та багатоядерні процесори, цифрові сигнальні процесори, спеціалізовані інтегральні схеми та програмовані логічні матриці. КФС можуть зазнавати атак, спрямованих не тільки на вбудовані системи і персональні комп'ютери, але й кіберзагроз, орієнтованих конкретно на КФС. Відомою є атака Stuxnet Worm на Іранську атомну електростанцію, які спричинила зараження вірусом великої кількості персональних комп'ютерів, що керували роботою станції. Вірус перехоплює і модифікує інформаційний потік між програмованими логічними контролерами марки SIMATIC S7 і робочими станціями SCADA-системи SIMATIC WinCC фірми Siemens. Цей вірус використовує чотири раніше не відомі вразливості системи Microsoft Windows, одна з яких – нульовий день (zero-day), спрямована на поширення за допомогою USB-flash накопичувачів. Вислизати від антивірусних програм вірусу допомагала наявність справжніх цифрових підписів (два дійсні сертифікати, випущені компаніями Realtek і JMicron) [3]. Більшість вразливостей обчислювальних платформ є наслідком відсутності довіри між основними системними компонентами під час їх взаємодій. Негативні наслідки атак посилюються взаємодією КФС з фізичним світом, у якому успішні атаки можуть поставити під загрозу людські життя. Відсутність довіри в системних компонентах обумовлена декількома факторами, зокрема труднощами перевірки, використанням "ненадійних компонентів".

Особливо треба звернути увагу на використання "ненадійних компонентів" у КФС (тобто компонентів, безпека яких не є гарантованою). Стандартні підходи уникнення загрози розробленням надійних додатків відповідно до суворих механізмів безпеки, таких як фізичний поділ потоку інформації, тепер використовують рідше через високу вартість. Такі методи можуть тільки зменшити кількість системних вразливостей, а не усунути їх всі. Більшість програмних і апаратних компонентів, що застосовуються у сучасних вбудованих системах, імпортуються з різних джерел і не можуть розглядатися як сертифіковані або надійні. Це зумовлює додаткові побоювання щодо здійснення навмисних шкідливих змін у компонентах. Такі умисні вразливості можуть входити у компонент на будь-якій стадії його виробництва або потрапити в нього разом з оновленням програмного забезпечення.

Забезпечення захисту сторонніх IP модулів є дуже складним завданням, оскільки зазвичай немає супровідної специфікації або "еталонного" прикладу, що працює. Ця проблема загострюється і може призвести до порушень безпеки системи, коли вбудований контролер складається з численних модулів, безпека яких не є гарантованою. Однак використання ненадійних компонентів у вбудованих контролерах неминуче.

Загалом можна виділити два основні способи апаратного захисту [11]:

1. Захист під час розроблення передбачає повну перевірку системи перед реалізацією. Такі методи надзвичайно дорогі з погляду часу і грошей і можуть виконуватись тільки над певним набором компонентів. Методи перевірки системи не можуть забезпечити перевірку всіх вразливих місць.

2. Захист під час експлуатації – передбачають виконання перевірки під час роботи системи. До системи можуть входити додаткові компоненти для забезпечення захисту, здебільшого це модулі шифрування і аутентифікації. Вони допомагають забезпечити цілісність інформації. Однак такі методи не забезпечують захист всіх компонентів системи, тому система може залишатися вразливою до непередбачених кіберзагроз.

Дослідження, пов'язані з апаратною безпекою, дуже важливі. Як правило, про вразливості системи дізнаються після процесу розроблення. Це стосується вбудованих систем, що використовуються у КФС. Постійне виправлення системних вразливостей вказує на необхідність вживання запобіжних засобів захисту під час проектування. Оскільки неможливо забезпечити стандартне рішення для всіх КФС, такі задачі потрібно розв'язувати під час розроблення конкретних систем.

Можна виділити такі основні завдання, пов'язані із загрозами апаратної безпеки:

1. Забезпечення захисту реконфігурованих систем, що містять ненадійні компоненти. Основне завдання полягає в тому, що необхідно перевіряти різноманітні запити від ненадійних систем, що передаються через мережеві канали [10].

2. Виявлення програм-шпигунів (Hardware Trojan Hourses, HRS) у "сторонніх" IP-ядрах (third-party IP cores, 3PIP), що містяться у кіберфізичних системах. Основна складність – це виявлення аномальної поведінки ненадійних компонентів, які розглядаються як чорні скриньки, і застосування належних контрзаходів у відповідь [11].

3. Зменшення ефекту кібератак на системи керування технологічними процесами. Основне завдання – це виявлення помилкової поведінки, спричиненої кібератакою, та запобігання наслідкам [12].

Забезпечення захисту реконфігурованих систем

Високий технологічний розвиток великої кількості IC (Integration circuit) протоколів привів до ідеї розробити новий тип апаратного забезпечення, відомий як *Cognitive radio* (CR) – це радіосистема, яка здатна сама отримувати дані про особливості свого використання і на підставі цих даних корегувати параметри своєї роботи. Ця система не є окремою службою радіозв'язку і може використовуватись як додаткова технологія у радіосистемі. Ці радіостанції динамічно адаптуються до різних протоколів скануванням широкого діапазону робочих частот.

CR-програмування безпеки є надзвичайно небезпечним, оскільки всі рівні стека протоколів можуть бути змінені, зокрема і апаратно реалізовані рівні. Система дозволяє власні зміни, однак апаратне забезпечення повинне перевіряти допустимість цих змін, а не покладатися виключно на правильність та цілісність програмного забезпечення. У разі одержання оновлень до таких пристроїв виникає небезпека здійснити навмисні шкідливі зміни. У сучасних засобах динамічна конфігурація апаратного забезпечення здійснюється на прикладному рівні програмного забезпечення. Всі програмні модифікації апаратної структури повинні проходити через контролер, що забезпечуватиме перевірку планованих змін.

Виявлення програм-шпигунів

Програми-шпигуни (Hardware Trojan Horses) – пристрій (або програма) в електронній схемі, таємно впроваджуваний до інших елементів, який здатний втрутитися в роботу обчислювальної системи. Результатом роботи програм-шпигунів може бути як повне виведення системи з ладу, так і порушення її нормального функціонування, наприклад, несанкціонований доступ до інформації, її зміна або блокування.

Загалом 3PIP ядра, залежно від використання, поділяються на три види:

1. Програмні – описуються за допомогою мов VHDL та Verilog і є найгнучкішими у використанні.

2. Фірмові – описані й синтезовані за допомогою спеціальних бібліотек.

3. Апаратні – описані на фізичному рівні, що використовуються як готові компоненти.

Програми-шпигуни можуть бути вбудовані у 3PIP ядра фірмою-розробником під час імплементації IP-ядра для того, щоб відстежити дані з інших систем. Виявлення таких програм-шпигунів є дуже складним завданням, оскільки фірма-виробник до специфікації основного коду додає і код програм-шпигунів. Якщо програма-шпигун є у IP-ядрі, то вона буде наявна і у всіх похідних IC (Integrated Circuit) компонентах.

3PIP ядра розглядаються, як чорні скриньки, у яких довіряти можна тільки функціональним характеристикам. Одним із можливих підходів перевірки на програми-шпигуни є написання тестів, спрямованих на перевірку функціональності пристрою.

Зменшення впливу кібератак на системи керування технологічними процесами

Системи керування технологічними процесами контролюють фізичні процеси і управляють ними на основі використання зворотних відгуків від систем, якими вони керують. Сенсорна інформація, зібрана за допомогою фізичних давачів, передається вбудованій системі для аналізу. Контролери процесу, як правило, розроблені з використанням ненадійних компонентів та 3PIP ядер, отже, є уразливими до кіберзагроз, спричинених відсутністю довіри до внутрішніх компонентів. Системи управління кібератаками широко використовуються у розробках спецслужб. Запобігання шкідливому проникненню є важким завданням через складність сучасних мережевих систем керування. Програми-шпигуни можуть потрапляти до КФС через мережу. Це призводить до можливості таємного зламу керуючих пристроїв. Помилкову поведінку такого пристрою треба виявити, перш ніж вона критично вплине на фізичний процес. Використовувані підходи щодо виявлення атак і помилок передбачають моніторинг стану операційних пристроїв на основі зворотних відгуків контролера, а також порівняння цих відгуків із вже наявними у системі.

Велика кількість успішних атак на системи керування технологічним процесом вказує на необхідність активних заходів безпеки. Найвідоміший приклад – це кібератака Stuxnet на Іранську атомну електростанцію.

Висновки

У роботі наведено огляд та основні характеристики КФС а саме: взаємодія з фізичними системами, наявність у кожному фізичному компоненті, взаємодія з різними мережами та ресурсами, динамічна реорганізація. Розглянуто способи апаратного захисту КФС: захист під час розроблення та захист під час експлуатації. Виокремлено основні завдання, пов’язані із забезпеченням апаратної надійності КФС, це: забезпечення захисту реконфігурованих систем, що містять ненадійні компоненти; виявлення програм-шпигунів; зменшення впливу кібератак на системи керування технологічними процесами.

Наукові результати, подані у цій статті, отримано в межах дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 – 31.12.2017, фінансово підтриманого Міністерством освіти та науки України.

1. Baheti R. and Gill H. Cyber-physical systems. The Impact of Control Technology. 2. Edward A. Lee and Sanjit A. Seshia. Introduction to Embedded Systems // A Cyber-Physical Systems Approach 2011. 3. Mohammed M. Farag, Architectural Enhancements to Increase Trust in Cyber-Physical Systems Containing Untrusted Software and Hardware // Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Engineering, 2012 Blacksburg, Virginia 4. Abhishek Gupta, Mohit Kumar, Future of all technologies // The Cloud and Cyber Physical Systems: International journal of enhanced

research in science technology & engineering – 2013. 5. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку. – Львів: Видавництво Львівської політехніки. – 2014. – С. 154–161. 6. Edward Ashford Lee, Sanjit Arunkumar Seshia, Introduction to Embedded Systems // A Cyber-Physical Systems Approach, Edition 1.5, LeeSeshia.org, 2014 7. Krishna Kumar. Venkatasubramanian, Security solutions for cyber-physical systems: a Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy, Arizona State University December 2009. 8. Ying-Chang Liang, Hsiao-Hwa Chen, J. Mitola, P. Mahonen, R. Kohno, J.H. Reed, and L. Milstein. Guest editorial – cognitive radio: Theory and application. Selected Areas in Communications // IEEE Journal on, 26(1):1–4, January 2008. 9. Tehranipooret M. al. Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection, Springer International Publishing, Switzerland. – 2014. 10. Lerner L. W., Farag M. M. and Patterson C. D. Run-time prediction and preemption of configuration attacks on embedded process controllers // In Security of Internet of Things (SecurIT), 2012 First International Conference on, August 2012. 11. Bloom Gedare, Leontie Eugen. Handbook on Securing Cyber-Physical Critical Infrastructure, Elsevier Inc. 2012. 12. *Alvaro A. Cardenas, Saurabh Amin, Challenges for securing cyber Physical Systems, Workshop on Future Directions in Cyber-physical Systems Security, DHS, 23, July, 2009.*