УДК 004.032.2

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

ПРОБЛЕМИ АПАРАТНОГО ЗАХИСТУ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

У роботі наведено основні відмінності кіберфізичних систем від вбудованих комп'ютерний систем, а також персональних комп'ютерів. Проаналізовано проблеми апаратного захисту у кіберфізичних системах.

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

HARDWARE SECURITY PROBLEMS IN CYBER-PHYSICAL SYSTEMS

The main differences between cyber-physical systems, embedded systems and personal computer are analyzed in this paper. The main hardware security problems in cyber-physical systems also considered in this work.

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 у інформаційної технологіях (IT). Надзвичайно швидкі персональні комп'ютери і портативні стільникові телефони, численні програми й інструменти, високошвидкісний інтернет по всьому світу і комп'ютерні мережі змінили спосіб, яким ми живемо. Вплив цієї революції, очевидно, впливає на кожен аспект нашого життя. Основна кількість 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 вбудовані системи є розгорнуті у фізичних системах. Тим не менш, є проблема взаємодії обчислень між кіберсистемою і фізичним світом, а також забезпечення захисту даних під час цієї передачі [1].

Способи апаратного захисту значно відрізняються від програмних чи мережевих. Зазвичай апаратне проектування і виробництво відбувається перед або разом із розробкою програмного забезпечення, як результат необхідно подбати про апаратну безпеку на ранніх стадіях розробки продукту [3]. Апаратні засоби контролюються програмним забезпеченням, яке в свою чергу керується кіберфізичними системами. У випадку зламу зловмисником апаратних засобів, механізми безпеки програмного забезпечення можуть виявитися марними [4]. Апаратне забезпечення має довшу тривалість існування ніж програмне, тому що програмне забезпечення може бути оновленим або заміненим на новий покращений варіант.

Постановка задачі

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 [5]. Саме тому, про потрібно дбати про безпеку апаратних засобів починаючи від їх проектування до утилізації.

Означення КФС

Термін кіберфізична система (КФС), був запропонований національним науковим фондом (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, де фізичний процес впливає 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 в середовищі з обмеженими ресурсами, КФС спрямовані на взаємодію обчислень із фізичним середовищем.

На даний час КФС можна знайти у таких галузях, як: аерокосмічна, автомобільна промисловість, хімічні процеси, цивільна інфраструктура, енергетика, охорона здоров'я, транспорт та розваги. Ця область відкриває нові можливості і створює додаткові задачі, такі як [5]:

1. Забезпечення взаємодії між розподіоеними кіберфізичними системами.
2. Забезпечення надійності і захисту інформації.
3. Забезпечення конторолю над гібридними ситемами.
4. Розробка архітектури.

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

Архітектура КФС

Як правило кіберфізичні системи побудовані у вигляді системи управління зі зворотним зв'язком по замкнутому циклу. Рисунок 1 ілюструє основну архітектуру КФС, де сенсори, виконавчі елементи (ВК) і контролери утворюють мережу елементів [7].

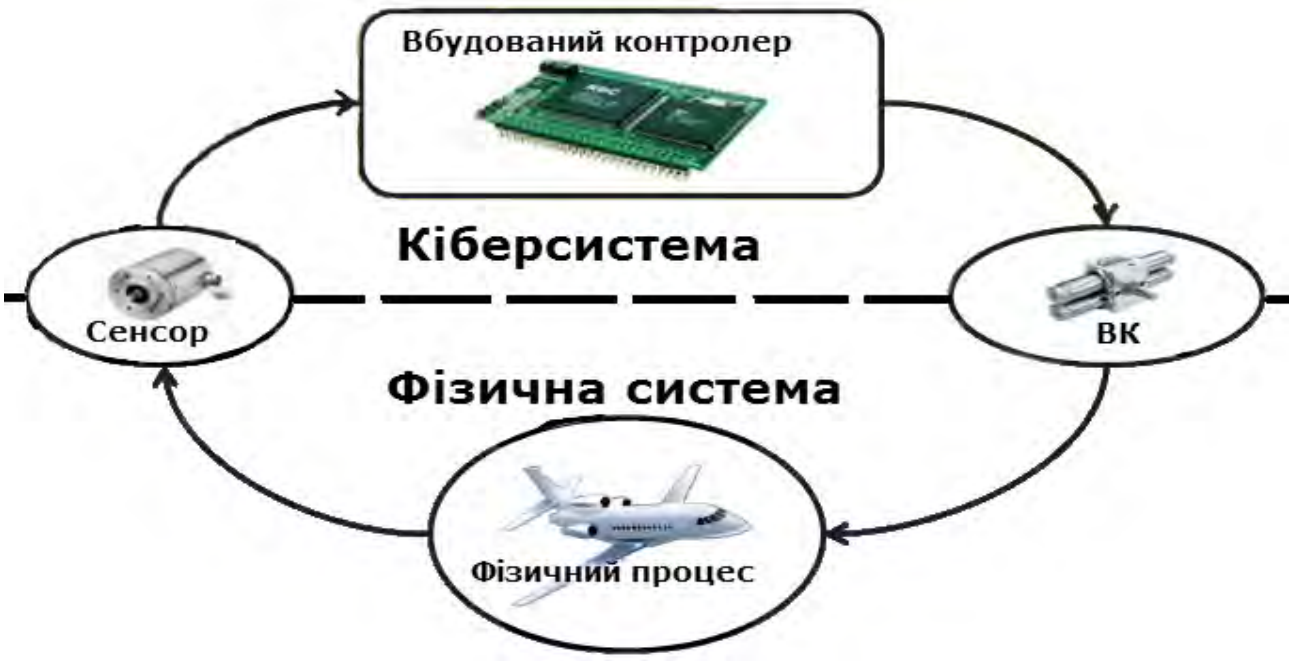

Рис.1 Архітектура кіберфізичної системи

Вбудовані контролери це обчислювальні системи, що включають набір компонентів, таких як процесори, пам'ять, пристрою вводу/виводу. Ця інфраструктура розподіляється у абстрактних рінях системи. Абстрактні рівні системи включають апаратні засоби, операційну систему (ОС), програмне забезпечення і дані. Сучасні компоненти характеризуються складністю функцій і взаємодій з даними, що проходять через різні рівні системи.

Для підвищення продуктивності розробки і скорочення 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 бути присутні у цих компонентах. Програми-шпигуни можуть бути вбудовані, як в апаратне так і програмне забезпечення. Так, як 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 володіють такими характеристиками [6].

1. Інтенсивна взаємодія з фізичними системами.
2. Присутність у кожному фізичному чи мережевому компоненті: програмне забезпечення міститься у всіх вбудованих системах або фізичних компонентах.
3. Взаємодія з різними мережами: мережі КФС, включають у себе дротові / бездротові мережі, Wi-Fi, Bluetooth.
4. Взаємодія з різноманітними ресурсами і їх властивостями.
5. Динамічна реорганізація / реконфігурація: КФС є дуже складними системами, і тому повинні мати адаптивні можливості.

Взаємодія з фізичним світом керує поведінкою КФС, зазвичай налаштованих, як системи управління зі зворотним зв'язком, де невелика зміна у поведінці фізичної системи індукує еквівалентну зміну у поведінці кіберсистеми, і навпаки. Взаємодія з фізичними системами має безперервну часову динаміку і відбувається у режимі реального часу. Крім того, фізичний світ є не зовсім передбачуваним і, отже, КФС повинні бути міцними, до несподіваних умов і збоїв підсистеми. Взаємодія з фізичним світом є фундаментальною відмінністю КФС від обчислювальних платформ загального призначення, де тільки користувачі можуть робити основні системні зміни. З точки зору безпеки, так як взаємодія між кібер і фізичними системами збільшується, фізичний світ стає більш вразливим до атак, що виникають у кіберсистемах. Ці проблеми безпеки обумовлюють необхідність забезпечення безпечного і надійного функціонування КФС.

КФС зазвичай включають у себе різні гетерогенні компоненти, які можуть розглядатися, як підсистеми, що включають в себе прості сенсори, дротові та бездротові комунікаційні та мережеві пристрої, а також вбудовані обчислювальні системи [7]. 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 також різноманітністю цілей і завдань. Ця різноманітність ресурсів, взаємодій і багатозадачність робить реалізацію КФС дуже складною. КФС є система з жорсткими зв'язками між

обчислювальною технікою і фізичними компонентами. Зв'язки між різними підсистемами, можуть бути фізично розділені і розподілені на великих відстанях. Це досягається за рахунок мережевих взаємодій у різних мережевих доменах. Це відрізняє КФС системи від традиційних вбудованих систем, що зазвичай зосереджені на одній платформі.

У таблиці 1 наведено порівняння властивостей КФС, вбудованих комп'ютерних систем та персональних комп'ютерів [9].

Таблиця 1

	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

Проблеми безпеки КФС

В останні кілька років, комп'ютерна безпека отримала значну увагу з боку наукового співтовариства. Були 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 в порівнянні з можливими ризиками ці проблеми не здаються такими суттєвими [10].

Основні проблеми безпеки є пов'язаними з використанням "ненадійних компонентів" у КФС (тобто, компонентів, безпека яких, не є гарантованою). Стандартні підходи уникнення загрози, шляхом розробки надійних додатків у відповідності із суворими механізмами безпеки, такими як фізичний поділ аналізу потоку інформації, стали використовуватись рідше через свою дорогу вартість. Такі методи можуть тільки зменшити кількість системних вразливостей, а не усунути всі з них. Більшість програмних і апаратних компонентів, що застосовуються у сучасних вбудованих системах імпортуються з різних джерел, і не можуть розглядатися, як сертифіковані або надійні. Це вводить додаткові побоювання, що можуть бути здійснені навмисні шкідливі зміни до компонентів, крім випадкових дефектів розвитку. Такі умисні вразливості можуть бути включені у компонент на будь-якій стадії його виробництва або потрапити разом з оновленням програмного забезпечення.

Забезпечення захисту сторонніх IP модулів є дуже складним завданням, оскільки зазвичай немає ні супроводжуючої специфікації або 'еталонного' працюючого прикладу. Ця проблема посилюється 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 є неминучим.

В загальному можна виділити два основні способи апаратного захисту[11]:

1. Захист під час розробки – передбачає повну перевірку системи, перед реалізацією. Такі методи є надзвичайно дорогим з погляду часу і грошей, і можуть бути здійсненні тільки над певним набором компонентів. Методи перевірки системи не можуть включати в себе перевірку всіх вразливих місць.
2. Захист під час експлуатації – передбачають виконання методів перевірки, щоб забезпечити гарантію з приводу деяких аспектів поведінки системи. До системи можуть бути додані додаткові компоненти для забезпечення захисту, в основному це модулі шифрування і аутентифікації. Вони допомагають забезпечити цілісність інформації. Тим не менш, такі методи не забезпечують захист всіх компонентів системи, і тому система може залишатися вразливою до непередбачених кіберзагроз.

Дослідження, пов'язані з апаратною безпекою, є дуже важливими. Як правило про вразливості системи дізнаються після процесу розробки. Це відноситься до вбудованих систем, що використовуються у КФС. Постійна виправлення системних вразливостей вказує на необхідність вжиття запобіжних засобів захисту під час процесу проектування. Оскільки не можливо реалізувати стандартне рішення для всіх КФС, такі задачі потрібно розв'язувати під час розробки конкретних систем.

Можна виділити такі основні проблеми пов'язані з загрозами апаратної безпеки:

1. Проблема забезпечення захисту реконфігурованих систем, що містять ненадійні компоненти. Основна проблема полягає в тому, що необхідно перевіряти різноманітні запити від ненадійних систем, що передаються через мережеві канали [10].
2. Проблема виявлення програм-шпигунів (Hardware Trojan Hourses, HRS) у "сторонніх" IP-ядрах (third-party IP cores, 3PIP), що містяться у кібер-фізичних системах. Основна проблема - це є виявлення аномальної поведінки ненадійних компонентів, які розглядаються, як чорні ящики і застосовувати належні контрзаходи у відповідь [11].
3. Проблема зменшення кібератак на системи управління технологічними процесами. Основна проблема - це виявлення помилкової поведінки, спричиненої кібератакою та попередження наслідків [12].

Забезпечення захисту реконфігурованих систем

Високий технологічний розвиток великої кількості IC (Integration circuit) протоколів привело до ідеї розробити новий тип програмного забезпечення, відомий, як *Cognitive radio* (CR) - це радіосистема, яка здатна сама отримувати дані про особливості свого використання, і на основі цих даних корегувати свої параметри роботи. Ця система не є окремою службою радіозв'язку і може використовуватись, як додаткова технологія у існуючій радіосистемі. Ці радіостанції динамічно адаптуються до фізичного рівня протоколів, шляхом сканування спектру, виявляючи можливості спектру з широкого діапазону робочих частот.

CR програмування являє собою проблеми безпеки, оскільки всі рівні стеку протоколів можуть бути змінені, в тому числі і апаратно-реалізовані шари. Система дозволяє власні зміні, однак апаратне забезпечення повинне перевіряти ці зміни, а не покладатися виключно на правильність та цілісність програмного забезпечення. При одержанні оновлень до таких пристроїв, виникає небезпека отримати 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 здійснених дій.

Виявлення програм-шпигунів

Програми-шпигуни (Hardware Trojan Horses) - пристрій в електронній схемі, що 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.

В загальному 3PIP ядра в залежності від використання, поділяються на три види:

1. Програмні – описуються за допомогою мов VHDL та Verilog і є найбільш гнучкими у використанні.
2. Фірмові – описані і 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 відслідковувати дані з інших систем. Виявлення таких програм-шпигунів є дуже складним завданням, так, як фірма виробник до специфікації основного коду, додає і код програм-шпигунів. Якщо програма-шпигун є присутньою у IP-ядрі, то вона буде присутньою у всіх похідних IC (Integrated Circuit) компонентах.

3PIP ядра розглядаються, як чорні ящики, де довіряти можна тільки функціональним характеристики. Одним із можливих підходів перевірки на програми- шпигуни є написання тестів, які спрямованих на перевірку функціональності пристрою.

Зменшення кібератак на системи управління технологічними процесами

Системи управління технологічними процесами контролюють і управляють фізичними процесами на основі використанням зворотніх відгуків від інших систем. Сенсорна інформація, зібрана за допомогою фізичних датчиків передається вбудованій системі для аналізу. Контролери процесу, як правило, розроблені з використанням ненадійних компонентів та 3PIP ядер, отже, є уразливими до кіберзагроз, спричених відсутністю довіри до внутрішніх компонентів. Системи управління кібератаками широко використовуються у розробках спецслужб, де успішні кібератаки можуть призвести до катастрофічних лих. Запобігання шкідливого проникнення є складною задачею через складність сучасних мережевих систем управління. Програми-шпигуни можуть потрапляти до КФС через мережу. Це призводить до можливості таємного зламу керуючих пристроїв. Помилкова поведінка такого пристрою, повинна бути виявлена, перш ніж вона критично вплине на фізичний процес. Існуючі підходи щодо виявлення атак і помилок включають в себе моніторинг стану операційних пристроїв на основі зворотніх відгуків контролера, а також порівняння цих відгуків із вже існуючими у системі.

Велика кількість успішних атак на системи управління технологічним процесом, вказує на необхідність активних заходів безпеки. Найбільш відомий приклад - це кібератака на систему управління технологічними процесами Stuxnet на Іранського атомній електростанцію.

Висновки

У роботі розглянуто основні задачі, що виникають при розробці кіберфізичних систем Також наведено огляд та основні характеристики КФС. Розглянуто основні проблеми захисту апаратного забезпечення та підходи їх вирішення.

*1.R. Baheti and H. Gill. 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 Видавництво Нац. ун-ту "Львівська політехніка", Львів, 2014 – 154с. 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. M. Tehranipooret al., Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection, Springer International Publishing, Switzerland – 2014. 10. L.W. Lerner, M.M. Farag, and C.D. Patterson. 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. Gedare Bloom, Eugen Leontie, 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*

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