УДК 004.032.2
О.З. Шологон
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

БЕЗПЕКА У КІБЕРФІЗИЧНИХ СИСТЕМАХ

У роботі проаналізовано різновиди атак та властивості безпечності у кіберфізичних системах. Для забезпечення збереження конфіденційності та захисту цілісності інформації розглянуто вимоги щодо криптогрфічних причтроїв у КФС.

Ключові слова: кіберфізичні системи, атаки,криптографія

SECURITY IN CYBER-PHYSICAL SYSTEMS

In the paper is analysed the types of attacks and security properties in the cyber-physical systems. To ensure the confidentiality and integrity of information considered to review cryptography requirenments of cyber-physical system.

Key words: cyber-physical systems, attacks, cryptography.

Вступ

Захист інформації завжди був предметом інтересу, і в наш час, коли ми використовуємо технології у більшості областей нашого життя, безпека є більш важливою, ніж коли-небудь. Інформаційні системи з кожним днем стають все складнішими і тому найменший витік інформації може стати фатальним. У зв’язку з цим сучасні дослідження спрямовані на знаходження систем які б змогли збалансувати поєднання фізичних і обчислювальних елементів. Такі системи називаються кіберфізичними системами (КФС) [1,2].

Термін кіберфізичні системи являє собою взаємодію між реальним світом та інформаційними системами. Основною метою кіберфізичних систем є контроль поведінки фізичних процесів частиною, яких вони є. КФС не є традиційними системами у режимі реального часу, вони надають додаткових властивостей класичними системам. Їх кібер і фізичні компоненти інтегровані для навчання та адаптації,самоорганізації і продуктивності.

Постановка задачі

На даний час головною проблемою постає надійна взаємодія систем управління з фізичними системами. В цілому відомо багато методів щодо забезпечення безпеки (аутентифікація, контроль доступу, цілісність повідомлень). Однак ці дослідження спрямовані більше на захист інформації, а не фізичних систем. Тому природним постає питання про захист таких систем від зламу.

Характеристики і принцип роботи КФС

Кіберфізичні системи мають застосування у багатьох областях, таких як: управління охорони здоров’я, автомобільне упралівння, електромережі, фізична інфраструктура (дороги, мости).

Незалежно від області застосування КФС мають такі основні характеристики [2]:

- *Залежність від середовища виконання.*

КФС дуже тісно пов’язані з середовищем в якому вони виконуються (фізичні процеси). Будь-яка зміна в поведінці середовища прозводить до зміни поведінки кіберфізичної системи.

- *Чітко визначені можливості*

КФС, як правило, складаються з декількох компонентів, які мають різні характеристики. Сенсори, які вбудовані в фізичні пристрої з метою моніторингу, мають обмежені можливості. В той час як програмні засоби, що керують цими сенсорами є більш потужнішими.

- *Мережевість*

КФС, на відміну від традиційних автономних вбудованих систем, вимагають мережевий зв'язок між компонентами для того, щоб забезпечити свої послуги.

Принцип роботи КФС

Принцип роботи кіберфізичних систем можна класифікувати на 3 етапи [3]:

1. Моніторинг

Головний аспект в КФС, який полягає в спостереженні за роботою середовища в якому працює КФС. Він також використовується для отримання відгуків щодо будь-яких дій які відбувалися в минулому з КФС. Це потрібно для того, щоб уникнути збоїв у системі у майбутньому.

2. Обробка даних

Стосується аналізу даних, зібраних в ході моніторингу, для того щоб дізнатися чи фізичний процес відповідає попередньо визначеним критеріям. У випадку, коли критерії не є задоволеними, коригувальні дії визначаються відповідно до інших успішно виконаних критеріїв.

3. Виконання

На цьому етапі здійснюється виконання дій, які були визначені на етапі обробки даних. При цьому поведінка КФС може бути змінена повністю.

Будь-яка кіберфізична система може виконуватись в одному з трьох можливих режимів: пасивний, пасивно-активний та активний. (Рис1.)

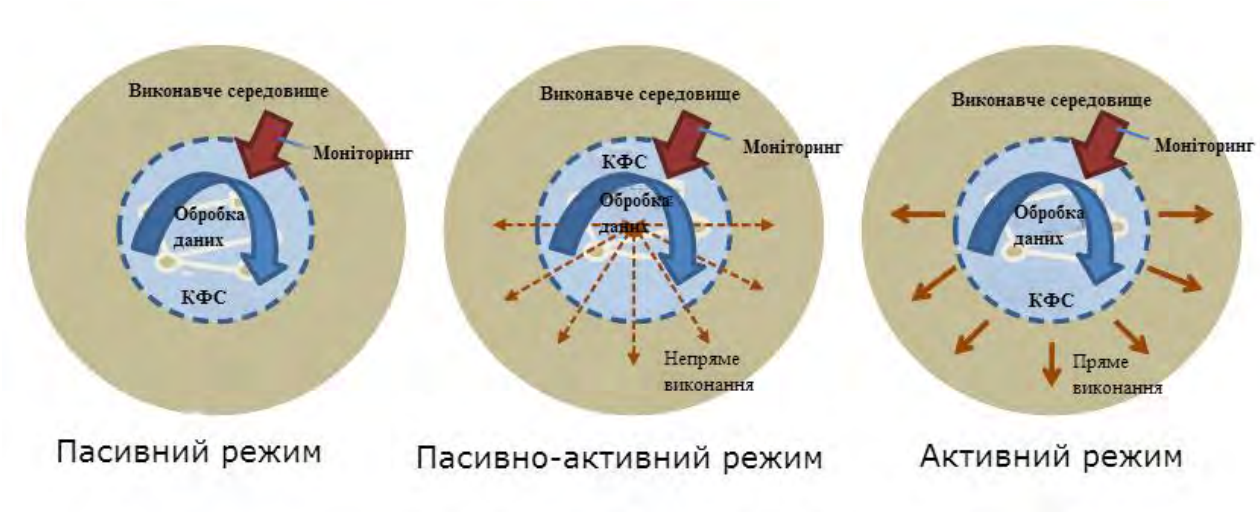

Рис1. Режими роботи КФС

Пасивний режим - у цьому режимі кіберфізична система не виконує ніяких дій, окрім збору інформації та контролю середовища. (Наприклад: медичні прилади.)

Пасивно-активний режим - у цьому режимі кіберфізична система контролює своє оточення (фізичний аспект). Якщо певна дія виконується не вірно, тоді відбувається непряме виконання шляхом зміни поведінки системи (кібераспект). Наприклад: дата-центри виконують smart-планування для того, щоб зменшити температурну шкалу в певних місцях

Активний режим – в цьому режимі кіберфізична система, як і в пасивно-активному режимі контролює своє середовище. Однак, коли певна дія виконується не вірно, тоді відбувається пряме виконання шляхом модифікації поведінки фізичного середовища. Наприклад: сисstми вентиляції приміщень.

Різновиди атак у КФС

Атака - це будь-яка спроба знищити, відключити, вкрасти або отримати несанкціонований доступ до системи [3].

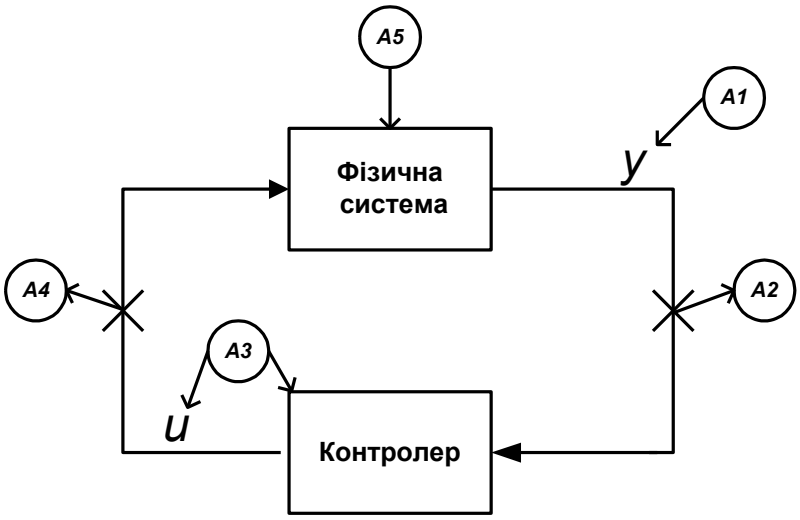

Рис2. КФ Атаки

Атаки у КФС (рис2.) можуть бути класифіковані наступним чином [4]:

1. A1 і A2 представляють *обманні атаки,* де зловмисник з сенсора або контролера відправляє хибне повідомлення $y \neq y$ або $u \neq u$. Неправдива інформація може містити неточні виміри, час або інформацію про відправника. У будь-який момент під час атаки система не знає про обман і припускає, що всі дані і послуги, отримані від зловмисника є законними. Також при такому виді атак зловмисник може перехопити будь-яку інформацію, передану в системі. Такі атаки здійснюються при наявності секретного ключа або за допомогою зламу сенсорів (A1) чи контролерів (A3).
2. A2 і A4 відображають DoS атаки. Зловмисник не дає контролеру отримувати інформацію з фізичної системи. У цьому випадку відбувається проникнення у комунікаційні канали. При цьому зловмисник може не тільки отримати доступ до інформації, але також змінити або видалити її. Це також може призвести до некоректного виконання і затримки ініціалізації конкретних послуг.
3. A5 це прямі атаки на КФС. З алгоритмічної точки зору не можливо забезпечити вирішення цих атак (окрім виявлення їх). Тому, значні зусилля повинні бути спрямовані на запобігання прямих атак на фізичні системи.

Хоча A5 атаки і є найбільш руйнівними, вони трапляються нечасто, тому при розробці систем захисту інформації слід звернути увагу на атаки A1-A4.

Вимоги щодо безпеки у КФС

Для того, щоб уникнути атаки на систему повинні бути дотримані такі вимоги безпеки.

Конфіденційність

Під конфіденційністю розуміється здатність приховувати дані [5]. Це зазвичай досягається за допомогою криптосистем. Криптосистема - це математична функція, яка перетворює (шифрує) вхідне повідомлення у зашифрований текст. При цьому зашифрований текст може бути перетворений у початковий стан тільки при наявності інверсної функції. Процес шифрування і розшифрування може відбуватися тільки за допомогою криптографічного ключа. Розшифрувати повідомлення практично не можливо, не знаючи точного значення ключа. Існують два типи криптографічних систем, які можуть бути використані для забезпечення конфіденційності: симетричні та асиметричні криптосистеми.

Під симетричними криптосистемами розуміються такі криптосистеми, в яких для шифрування і розшифрування використовується один і той же ключ [6]. Недоліком цих систем є те, що при втраті або викраденні ключа конфіденційність системи втрачається. Деякі з відомих алгоритмів, які використовують симетричний ключ є AES[7] і RC5[8].

У асиметричних криптосистемах для шифрування і розшифрування використовуються різні ключі зв'язані між собою деякою залежністю [9]. При цьому встановити один ключ знаючи інший, з обчислювальної точки зору, дуже складно. Один із ключів (наприклад ключ шифрування) може бути загальнодоступним, і в такому випадку проблема отримання загального секретного ключа відпадає. Відомі такі асиметричні алгоритми: RSA, Діффі-Хеллман.

Цілісність

При забезпеченні цілісності даних потрібно враховувати здатність виявляти будь-які зміни, які внесені у передане повідомлення. Це зазвичай робиться за допомогою хеш функції.

Хеш функція на вхід приймає дані, цілісність яких потрібно забезпечити, і на вихід подає випадкове значення фіксованої довжини яке називається збірка [9]. Оскільки ця функція є односторонньою, то при найменшій зміні вхідних даних, результат буде іншим. Для асиметричних сценаріїв, хеш функція використовується для отримання даних, які зашифровані за допомогою приватного ключа – цифрового підпису. При перевірці цілісності даних хеш функція обчислюється за допомогою відкритого ключа, після чого розшифрований текст порівнюється з наявним. Відомі такі алгоритми: MD5[10], SHA[11].

Аутентифікація

Аутентифікація встановлює рівень довіри між системами, що потім є основою всієї подальшої комунікації. В інтерактивних системах аутентифікація забезпечує розпізнавання системи. Деякими добре відомими методами є: цифрові сертифікати, біометричні показники, взаємодії запит-відповідь.

Авторизація

Враховуючи особу суб'єкта, що взаємодіє з системою, авторизація визначає і керує системними даними за допомогою моделі управління доступом. У своїй основній формі вона працює наступним чином:

1) Особа, яка хоче використовувати об'єкт в системі робить запит.
2) Модель управління доступом приймає запит і ідентифікує особу. Після чого надає їй певні привілеї на основі чітко визначених правил.
3) Якщо запит відповідає привілеям, тоді доступ дозволений.

Криптографічні вимоги у КФС

З наведеного вище можна зробити висновок, що для збереження конфіденційності та захисту цілісності інформації, основною вимогою є використання криптографічних методів.

Процес криптографічного закриття даних може здійснюватись як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, проте їй властиві і переваги: висока продуктивність, простота, захищеність. Програмна реалізація більш практична, і дозволяє більшу гибкість у використанні.

Незалежно від способу реалізації для сучасних криптографічних систем захисту інформації складені наступні вимоги [6,12]:

- Знання алгоритму шифрування не повинно знижувати криптостійкість шифру. Ця вимога була сформульована в XIX ст. Керкхоффом і поділяє криптосистеми на два види: загального використання (алгоритм є доступним потенційному порушнику) і обмеженого використання (аглоритм тримається в таємниці). Всі масово використовувані криптосистеми повинні відповідати другій вимозі.
- Вибір криптографічної технологій має задовільняти вимогам надійності.
- Зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа.
- Шифр повиннен бути стійким навіть коли зловмиснику відома достатня кількість вхідних даних і відповідних їм зашифрованих даних.
- Незначна зміна ключа або вихідного повідомлення повинно приводити до суттєвої зміни вигляду зашифрованого тексту.
- Структурні елементи алгоритму шифрування повинні бути незмінними
- довжина шифрованого повідомлення повинна бути рівною довжині вихідного повідомлення.
- Додаткові біти, які вводяться в повідомлення в процесі шифрування повинні бути повністю і надійно приховані в шифрованому повідомленні.
- будь-який ключ із множини можливих повинен забезпечувати рівну криптостійкість.
- Не повинно бути простих і легко встановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування
- Число операцій необхідних для розшифрування інформації шляхом перебору можливих ключів повинно мати чітку нижню оцінку, і повинно або виходити за межі можливостей сучасних комп’ютерів або потребувати використання дорогих обчислювальних систем.
- Довжина шифрованого повідомлення повинна бути рівною довжині вихідного повідомлення.
- Будь-який ключ із множини можливих повинен забезпечувати рівну криптостійкість.

Висновки

У даній роботі наведено основні характеристики та принципи роботи кіберфізиних систем. Також описано різновиди атак у КФС, властивості безпечності та криптографічні вимоги у КФС.

1.Мельник А. О., Кіберфізичні системи: проблеми створення та напрями розвитку, Видавництво Національного університету "Львівська політехніка", Львів, 2014 -154с. 2. Laura Vegh,Liviu Miclea, Securing Communication in Cyber-Physical Systems using Steganography and Cryptography,Technical University of Cluj-Napoca, Faculty of Automation and Computer Science, Romania,June 2014. 3. Krishna Kumar Venkatasubramanian,Security solutions for cyber-physical systems, Arizona State University, December 2009; 4.Alvaro A, Cardenas Saurabh Amin, Shankar Sastry, Secure Control: Towards Survivable Cyber-Physical Systems, University of California, Berkeley, August 2013;5. Saddek Bensalem,Roberto Passerone,Alberto Sangiovanni-Vincentelli,CPS Methods and Techniques,Project co-funded by the European Union's Seventh Framework Programme,July 2013 6. Elliptic Curve Cryptographic Co-Processor Components for Security On medical Embedded Systems;7. J. Daemen and V. Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer Verlag, 2002. 8 R. L. Rivest. The RC5 encryption algorithm. pages 86 – 96, 1995. Workshop on Fast Software Encryption..9.Баричев С.Г., Серов Р.Е. Основы современной криптографии, М.: Горячая линия — Телеком, 2002. — 175 с;10. R. L. Rivest. The md5 message-digest algorithm (rfc 1321), 1992;11. W. Diffie and M. E. Hellman. New directions in cryptography. ieee transactions on information theory. IEEE Transactions on Information Theory, 22(6):644–654, 1976. 12.Swapna Iyer,Cyber Security for Smart Grid, Cryptography, and Privacy,Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793, USA,July 2011.

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.