Моделювання можливих загроз інформаційної безпеки в системах з використанням мікроконтроллерів AVR

Олексій Ляшенко, Олег Журіло

Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА,
м. Харків, пр.Науки, 14
E-mail: oleksii.liashenko@nure.ua

This paper presents the results of a study of the applicability of elliptic cryptography algorithms on microcontrollers of the AVR architecture. A review of possible threats to the security of information flows for microcontrollers is performed.

Ключові слова – мікроконтролер, інформаційна безпека, моделі загроз, еліптичні криві.

I. Вступ

В рамках роботи проводиться дослідження можливостей реалізації асиметричних криптоалгоритмів високого рівня безпеки на пристроях з дуже обмеженими ресурсами, а саме - реалізація криптографічного модуля на еліптичних кривих для пристрою архітектури AVR.

II. Аналіз захищеності інформаційних потоків при використанні мікроконтролерів AVR

Найбільш цікавими для зловмисників системами з застосуванням AVR є СКУД, системи телеметрії, контролю та обліку, а також автомобільна електроніка. Решта сфери застосування мікроконтролерів даного сімейства також вимагають захисту, але при цьому наслідки їх злому є набагато менш критичними і вигідними, а отже, і менш привабливими для порушників.

Складністю для захисту AVR-пристроїв є їх обмеженість в ресурсах ЦП і доступної пам'яті за сучасними мірками. Навіть прості мобільні телефони давно мають велику обчислювальну потужність. Але навіть на обмеженому просторі можна використовувати такі методи захисту, як шифрування даних, забезпечення автентифікації і забезпечення цілісності даних. Підлаштовуючи апаратну частину для максимальної оптимізації обчислювальних витрат, обсягу пам'яті і споживання енергії, на вільних обчислювальних потужностях можливе використання симетричних (AES, 3DES - підтримуються апаратно в Atmel AVR XMEGA, можлива програмна реалізація, але вона працює на порядок повільніше) і асиметричних криптоалгоритмів (RSA , DH, ECC), обчислення контрольної суми (CRC підтримується апаратно в мікроконтролерах сімейства Atmel AVR XMEGA), використання криптографічних хеш-функцій, комбінація вищевказаних методів.

Основними засобами забезпечення безпеки є програмне або апаратне використання симетричних криптоалгоритмів і криптографічних хеш-функцій, застосування ЕЦП, розвивається використання асиметричних криптоалгоритмів. Atmel для полегшення роботи над захистом даних і оптимізації організації даного захисту, а також для збільшення швидкодії вбудувала в свою провідну лінійку 8-бітних мікроконтролерів AVR XMEGA апаратні реалізації захисних алгоритмів. Користувач при необхідності може вибирати між симетричними алгоритмами шифрування AES і 3DES, а також між контрольними сумами CRC-16 і CRC-32.

III. Застосування еліптичної криптографії на AVR

Асиметрична криптографія незамінна при вирішенні завдання забезпечення шифрування в ситуації, коли між сторонами відсутній взаємна довіра при прийомі інформації.

Одними з найбільш швидких, економічних і прогресивних асиметричних криптоалгоритмів вважаються алгоритми, засновані на еліптичній криптографії [1].

Характеристики алгоритмів еліптичної криптографії можна представити наступним чином. Еліптична крива – це безліч точок (x, y), що описуються рівнянням: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + +a_6$.

Дане рівняння може розглядатися над довільними полями, і кінцевими полями в тому числі. В такому випадку рішенням рівняння буде безліч окремих точок, а не лінія, що представляє для криптографії інтерес, у зв'язку з можливістю програмної реалізації.

Для використання еліптичних криптоалгоритмів повинні бути узгоджені параметри, що визначають еліптичну криву - набір параметрів протоколу.

Крипостійкість всіх заснованих на еліптичних кривих алгоритмів забезпечується на відсутності субекспоненціальності алгоритму розв'язання задачі дискретного логарифмування в групах їх точок. Складність рішення також визначається порядком групи точок еліптичної кривої.

Існує досить велика кількість алгоритмів еліптичної криптографії, але далеко не всі з них є популярними. Найбільш часто вживаними в захищених системах алгоритмами еліптичної криптографії можна назвати: протокол отримання секретного ключа ECDH, алгоритм ECIES, алгоритм для створення цифрового підпису ECDSA, алгоритм для створення цифрового підпису ECSS.

IV. Моделі загроз та шляхи протидії

Основними загрозами безпеці переданої з мікроконтролера та на нього інформації є [2]:

– перехоплення переданих даних зловмисником;

− аналіз інформації, що передається;
− зміна інформації, що передається;
− глушіння потоку інформації.

Глушіння потоку інформації, а також її перехоплення є загрозами, які перебувають на найнижчому, фізичному, рівні мережевий моделі. Також на даному рівні можна розглянути таку загрозу, як отримання зловмисником фізичного доступу до мікроконтролеру.

Криптографічними алгоритмами можна забезпечити тільки частковий захист від другої загрози, це можливо організувати шляхом спеціального розподілу ключів. Головним в даному випадку дією, спрямованою на забезпечення інформаційної безпеки, буде організація фізичного захисту, яка не дозволяє порушнику дістатися до пристрою.

Для захисту ж від зловмисника з потоком інформації слід налаштовувати фізичні параметри бездротового приймача-передавача даних або організовувати фізичний захист для дротового каналу зв'язку.

Решта загроз розташовуються на мережевому рівні мережевий моделі, і криптографічні алгоритми стають основним засобом захисту та протидії їм. Автентифікація і схеми розподілу ключів дозволяють обмежити в доступі до вузлів мережі несанкціонованих особистостей, які є зловмисниками, доступ отримують тільки перевірені користувачі. Другим же засобом інформаційного захисту є шифрування. Шифрування дозволяє зберегти в секреті передаються по каналах дані в тому випадку, якщо порушник має доступ до каналів.

V. Вибір базового ядра AVR

В силу того, що архітектура AVR є досить складною структурою, а також зважаючи на наявність вільно розповсюджених реалізацій ядер AVR для ПЛІС, було прийнято рішення використовувати сторонню реалізацію, виконану на мові опису апаратури VHDL. Таких було проаналізовано три:

− AVR Core - найбільш відома і часто використовувана реалізація. Являє собою Мікроконтроллерні ядро, сумісне з Atmel ATmega103, має такі ж набір і таймінг інструкцій, як це було зроблено мікроконтролер, прийнятий за зразок для моделювання. Дане ядро розглядалося в якості основного варіанту для запуску на ПЛІС, проте було виведено з роботи.;

− AVRTurnin - дана реалізація могла бути залишена в роботі як другорядна в силу своєї малої обчислювальної здатності, однак для роботи з криптографічними алгоритмами вона має занадто малими можливостями зберігання даних - всього 16 КБ постійної пам'яті і 1кб оперативної;

− pAVR - проект, який реалізує AVR-сумісний мікроконтролер, який не має конкретного зразка для моделювання. Метою реалізації було створення максимально потужною реалізації AVR. Побудований за даною технологією процесор приблизно в 3 рази швидше оригінального ядра.

VI. Результати використання еліптичної криптографії на мікроконтролерах

Результати дослідження показали, що використання еліптичної криптографії на мікроконтролерах архітектури AVR, можливо і піддається реалізації, незважаючи на велику обчислювальну складність еліптичних алгоритмів. Час на виконання криптографічних операцій, на жаль, дуже великий, тому звернення до реальних AVR-мікроконтролерів, що використовують алгоритми еліптичної криптографії, має проводитися не частіше, ніж раз в 30 секунд. У разі застосування софт-реалізацій AVR на основі ПЛІС, що володіють можливістю збільшення максимальної тактової частоти ЦП більш ніж в 3 рази в порівнянні з оригіналом, даний період часу може бути скорочений к співвідношенню використовуваних частот ЦП.

За результатами вимірювань можна зробити висновок, що використання еліптичної криптографії на AVR зажадає близько 39 КБ пам'яті програм і 5,5 КБ пам'яті даних. Вільними на мікроконтролерах сімейства ATmega128 залишаться 89 КБ пам'яті програм і 2,5 КБ пам'яті даних, що дозволяє організувати виконання додаткових операцій на мікроконтролері паралельно з використанням еліптичної криптографії.

Висновки

У роботі було проведено моделювання роботи мікроконтролера, були реалізовані алгоритми шифрування і ЕЦП високого рівня безпеки, засновані на ідеях еліптичної криптографії, а також проведені заміри продуктивності алгоритмів і використання ними доступної пам'яті.

Як показали порівняльні вимірювання з асиметричними алгоритмами і симетричними алгоритмами, використання алгоритмів еліптичної криптографії для підвищення рівня інформаційної безпеки на мікроконтролерах архітектури AVR можливо, не дивлячись на високу обчислювальну складність, але тільки в складі систем, які не потребують передачі даних частіше ніж один раз на 30 секунд. Застосування традиційних асиметричних алгоритмів шифрування на подібних мікроконтролерах можливо тільки при використанні рідкісних флагманських моделей з 32 КБ пам'яті даних через високе її споживання цими алгоритмами.

Література

[1] Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування. / Горбенко І. Д., Горбенко Ю. І. // ХНУРЕ, Приват. акціонер. т-во "Ін-т інформ. технологій". - Х. : Форт, 2013. - 878 с.

[2] Ruchika Markan. Literature Survey on Elliptic Curve Encryption Techniques / Markan Ruchika, Kaur Gurvinder // International Journal of Advanced Research in Computer Science and Software Engineering. 2013. – № 3. С. 906-909.