УДК 004.056.55

АНАЛІЗ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ ДЛЯ АВТОСИГНАЛІЗАЦІЇ

Д. І. Матяш[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі представлено аналіз систем автосигналізації, способів їх злому, використовуваних алгоритмів і криптографічних протоколів та їх захищеності для формування уявлення про сучасний стан систем автосигналізації.

Ключові слова: автосигналізація, автентифікація, протокол автентифікації, захищеність

Вступ

Велика кількість матеріальних цінностей, що знаходяться у публічних місцях, потребує ретельного захисту від спроб заволодіти цими цінностями особами, що не мають на це законних підстав. Отже, процедури перевірки справжності особи, що намагається отримати контроль над цінностями, є надважливими компонентами різних систем захисту та потребують ретельного аналізу та, можливо, модернізації під сучасні стандарти, потреби та виклики.

Практичне застосування систем автентифікації, що будуть проаналізовані у цій роботі – це застосування їх у системах захисту автомобіля від угону, крадіжки компонентів чи речей, що у ньому знаходяться, так званих автосигналізаціях. У зв'язку з високою розповсюдженістю автомобілів у нашому повсякденному житті та постійними все більш технічно та програмно досконалими атаками зловмисників на системи захисту автомобілів, дослідження протоколів автентифікації, що використовуються в сучасних автосигналізаціях та розробка більш криптостійких протоколів є надважливою задачею та має велике практичне застосування.

Наслідками злому чи сканування захисних пристроїв автомобіля часто стають значні фінансові збитки. Тому однією з головних проблем використання протоколів автентифікації у автосигналізіцвях є хороша криптостійкість алгоритму та неможливість його злому за адекватний час.

Отже, метою і завданням даної роботи є аналіз і детальне вивчення протоколів та методів автентифікації, які використовуються в автомобільних сигналізаціях; також аналіз методик та засобів удосконалення існуючих та створення більш крипостійкого алгоритму захисту.

1. Основні поняття

Автосигналізація – електронний пристрій, встановлений в автомобіль, призначений для його захисту від угону, крадіжки компонентів даного транспортного засобу або речей, що знаходяться в автомобілі.

Автентифікація – процедура встановлення справжності суб'єкта за пред'явленим їм ідентифікатором. Найбільш використовуваний спосіб автентифікації – парольна, тобто здійснювана на основі володіння користувачем певної конфіденційної інформації.

Протоколи автентифікації – категорія криптографічних протоколів, які забезпечують надійну автентифікацію особи.

2. Сучасний стан систем автосигналізації та способи злому

Автомобільна сигналізація складається, як правило, з основного блоку, приймально-передавального пристрою з антеною, брелоку (віддаленого блоку керування), датчика удару, датчиків відкриття дверей, капоту та багажнику, сервісної кнопки і індикатора у вигляді світлодіода. Автосигналізації бувають зі зворотним зв'язком, тобто брелок-пейджер інформує про стан автомобіля.

Відносно прості та недорогі системи використовують однонаправлений канал зв'язку, що призводить до низької безпеки системи в цілому. В таких пристроях найчастіше кодова комбінація не змінюється взагалі або кількість варіантів таких змін сильно обмежена. Системи зі зворотнім каналом зв'язку мають значно кращій рівень захисту але, внаслідок своєї високої вартості, знайшли широке комерційне застосування відносно недавно.

Виходячи з цього можна сформулювати два основні правила, які дозволять системі дистанційного керування з односпрямованим каналом зв'язку називатися безпечною:

- Число можливих кодових комбінацій має бути великим;
- Кодер не повинен формувати один і той же код двічі.

В сучасних системах автосигналізацій використовується широко відома в криптографії технологія аутентифікації за одноразовими паролями через незахищений канал з використанням так званих однонаправлених функцій – криптографічно стійких хеш-функцій чи симетричних блочних алгоритмів шифрування.

Діалоговий код – спеціальний спосіб кодозахищеності автосигналізацій. Використовує для ідентифі-

кації брелока широко відому в криптографії технологію аутентифікації через незахищений канал.

Отримавши сигнал, система переконується, що він посланий зі «свого» брелока, причому це відбувається не одноразово, а в діалозі. У відповідь на перший сигнал система посилає на брелок запит у вигляді псевдовипадкового числа, який обробляється брелоком за спеціальним алгоритмом і відсилається назад. Сигналізація (а саме блок керування) обробляє свою посилку за тим же алгоритмом, порівнюючи отриману відповідь зі своїми даними. Якщо вони збігаються, команда виконується, а на брелок відправляється підтвердження.

Для злому (підміни кодової радіопосилки) автосигналізацій зловмисники використовуються кодграббери («code grabber»). Розрізняють три типи подібних пристроїв: кодграббер для статичних кодів, кодграббери на принципі кодопідміни та алгоритмічні (іноді їх називають «мануфактурними»).

Для більш ранніх систем автосигналізацій, що використовують статичний код, досить пристрою, який перехоплює цей код і запам'ятовує його.

Для кодграбберів, що вікористовують принцип кодопідміни, характерний алгоритм роботи, що вимагає повторного натискання власником кнопок брелока, використовуючи частково одночасно радіозаглушення і перехоплення посилки брелока.

Алгоритмічний кодграббер – пристрій, який розпізнає по цифровій посилці брелока тип сигналізації, тобто виробника пристою, і, використовуючи так званий «мануфактурний код», стає клоном (повним дублікатом) брелока власника. Цей принцип застосовується до автосигналізацій, що використовують критпостійкі алгоритми (KeeLoq та інші).

3. Використовувані протоколи автентифікації, аналіз їх захищеності

Переважна більшість систем автосигналізації працюють на мікросхемах Microchip Technology, що реалізують алгоритм KeeLoq, який наразі є фактично стандартом індустрії. KeeLoq є блоковим алгоритмом шифрування, що використовує 32-бітний блок і 64-бітний ключ.

Основні визначення технології KeeLoq

Серійний номер – в кожен передавач при виготовленні програмується 28 або 32 бітний унікальний серійний номер.

Секретний ключ – це 64-бітний код, зформований функцією генератора ключів з 28/32-бітного серійного номера або 32/48-бітного «кодового зерна» і 64-бітного заводського номера. Секретний ключ не може бути зафіксований ззовні, він ніколи не передається.

«Кодова зерно» – це 32/48-бітове значення програмується в кодер передавача. При цьому половина кодового значення використовується при генерації ключа. Значення "кодового зерна"передається тільки після натискання на ньому певної комбінації клавіш і може вимикатися по закінченні процесу навчання.

Генерація секретного ключа – використовується для формування унікального номера передавача. При генерації використовується серійний номер і «кодове зерно». Генерація коду за нелінійним законом проводиться програматором при програмуванні кодера.

Заводський ключ – програмується в декодер при виготовленні пристрою, і використовується для генерації секретного ключа.

Нормальний режим навчання – приймач використовує інформацію, отриману зі звичайної кодової посилки для отримання секретного ключа передавача, визначення величини відмінності і лічильника синхронізації. Вся інформація, отримана від передавача, зберігається.

Безпечне навчання – передавач активізується через певну комбінацію кнопок, після чого він передає 32- або 48-бітну кодову посилку ("кодове зерно"), яка може використовуватися при генерації ключа як його частину.

Величина дискримінації – являє собою 12-бітну фіксовану частину зашифрованого слова. Дана величина використовується приймачем при розшифровці.

Лічильник синхронізації – 16-бітний лічильник, який збільшує своє значення на одиницю щоразу, коли відбувається активація передавача. Приймач запам'ятовує значення лічильника у внутрішній пам'яті і порівнює його із значенням, отриманим з попередньої посилки. Якщо значення потрапляє в робоче вікно, то код приймається.

Кодери

Формувачі динамічно змінюваного коду (hopping code) KeeLoq призначені для односпрямованих систем дистанційного керування. У функції кодера входить тільки формування кодової посилки, розробнику системи дистанційного керування необхідно подбати про організацію каналу зв'язку. Ініціалізація кодера на передачу коду відбувається після натискання на кнопку пульта дистанційного керування. Для радіомаяка на основі технології KeeLoq ініціалізація передачі коду може відбуватися і під впливом зовнішнього електромагнітного поля.

У технології KeeLoq використовується система реверсивної ідентифікації за принципом «свій – чужий». На основі серійного номера передавача і заводського ключа приймача за спеціальним алгоритмом формується 64-бітний секретний ключ та записується у кодер на етапі його програмування. Секретний ключ не може бути отриманий з кодера, і він ніколи не передається по каналу зв'язку.

При кожній ініціалізації кодера (натискання на кнопку пульта дистанційного керування) формується кодова послідовність, в яку входить 32-бітний hopping code, отриманий з 64-бітного секретного ключа. Hopping code унікальний для кожної нової кодової послідовності.

У технології KeeLoq кодова послідовність повторитися більш ніж через 65 тисяч команд. Якщо пульт дистанційного керування використовувати 8 разів на добу, то пройде 22 роки, перш ніж та ж сама кодова комбінація повториться знову. При цьому повторна

передача коду (наприклад за допомогою пристрою перехоплення коду) не викличе спрацьовування системи.

Алгоритм KeeLoq використовує особливу систему синхронізації. Прийнята посилка декодируется і зберігається в пам'яті. Наступні посилки вважаються істинними, якщо вони лежать в зоні 16 можливих наступних кодових комбінацій. Це зроблено для того, що б не відновлювати синхронізацію кожного разу після натискання кнопки на пульті управління в зоні недосяжності для приймача. У разі виходу кодової комбінації із зони 16 варіантів, необхідно двічі натиснути кнопку на пульті управління, і синхронізація буде відновлена. Операція синхронізації повністю прозора – користувач навіть не буде знати про те, що синхронізація була втрачена і відновлена.

При простій апаратній реалізації протокол KeeLoq має високий рівень захисту, порівняний з алгоритмом DES. Закладена у кріптосхему довжина секретного ключа в 64 біта робить нереалістичною атаку лобовим розкриттям, тобто перебором всіх можливих ключових комбінацій. Підібрати ключ виходячи з перехопленої інформації неможливо. Існують випробування систем, які можуть бути використані для перевірки характеристик безпеки алгоритму кодування і також для передбачення наступного переданого коду. На даному алгоритмі були перевірені такі види атаки як лавинний ефект (Avalanche Effect) і його підмножини. Результат перевірки дав хороший показник ефективності системи безпеки.

1. Лавинний ефект (AE) Блоковий шифр задовольняє критеріям AE, якщо при заміні одного інформаційного біта, в середньому змінюється половина переданих бітів. Стосовно до алгоритму KeeLoq це означає що зміна одного біта у функції та / або інформації синхронізації змусить в середньому змінитися 16 з 32 бітів в переданому коді.

2. Строгий Лавинний Критерій (SAC) Щоб протокол задовольняв даному критерію, необхідно, щоб на один змінений біт зашифрованої інформації змінювалося половина вихідних інформаційних бітів. Отже, можливість вгадування будь-якого біта інформації дорівнює 0.5, а ймовірність правильного вгадування всієї 32-розрядної інформаційної посилки дорівнює одна до 4,300,000,000. На вхід алгоритму, при проведенні тестів, подавалося випадкове значення 64-бітного ключа, а також вміст лічильника Грея, який змінювався, починаючи з нуля. У кожному випадку значення, що з'являється на виході алгоритму порівнювався з вхідною величиною (SAC тест) або з попереднім кодом (AE тест). Обидва випадки дали такі результати: при AE тесті середня величина змінюваних бітів виявилася рівною 16.0 (50 відсотків) із стандартним розкидом значень 2.83 (8.8 відсотків). При SAC тесті зміна одного вхідного біта дає зміна вихідного значення в середньому на 50 відсотків, з середнім розкидом значень в 8.8 відсотків.

Висновки

Отже, в роботі проведено аналіз систем автосигналізації, способів їх злому, використовуваних алгоритмів і криптографічних протоколів та їх захищеності. Проаналізовано стандарт індустрії – криптографічний протокол KeeLoq, який за результатами тестування підтвердив високі показники криптозахищеності системи. Очевидні переваги використання технології KeeLoq, вартість якої порівнянна з ціною систем на основі фіксованого коду – можливість будувати конкурентноздатні системи з високим рівнем безпеки.

Перелік використаних джерел

1. Bogdanov Andrey «Attacks on the KeeLoq Block Cipher and Authentication Systems». — June, 2007.
2. Технична документація TB003 компанії Microchip Technology Incorporated,USA.