

## ПОКРАЩЕННЯ БЕЗПЕКИ СИСТЕМ ДИСТАНЦІЙНОГО КЕРУВАННЯ

© Нємкова О. А., Чаплига В. М., Шандра З. А., 2013

**Розглянуто питання безпеки систем дистанційного бездротового зв'язку для специфічних випадків роботи. Огляд існуючих систем безпеки показав необхідність посилення процедури автентифікації. Запропоновано протокол взаємної суворой автентифікації, якому передують процедура ідентифікації контрольним сигналом. Використано протокол “запит – відповідь” з динамічним кодом.**

**Ключові слова:** безпека бездротового зв'язку, взаємна автентифікація, автосигналізація, мануфактурний код, автобрелок.

**The paper considers the security of wireless remote for specific cases work. Review of existing security systems has shown the need to strengthen authentication. A strict protocol of mutual authentication procedure is proposed by identification control signal. Protocol used “request – response” with dynamic code, touch memory.**

**Key words:** wireless security, mutual authentication, car alarm, the manufacturing code.

### Вступ

Безпека систем дистанційного бездротового керування ґрунтується на успішному вирішенні трьох питань: по-перше, захисту від під'єднання до мережі нелегальних користувачів, по-друге, запобігання несанкціонованому доступу до ресурсів мережі, по-третє, підтримки цілісності та конфіденційності даних, переданих через радіоканали. Сьогодні для вирішення двох перших питань застосовують процедури автентифікації (Authentication), авторизації (Authorization) та адміністрування (Accounting) – процедури AAA, стандарт IEEE 802.11, [1]. Третє питання вирішується шифруванням даних: поточним або блочним, а також тунелюванням.

Як відомо, автентифікація – це процес встановлення автентичності абонента за його ідентифікатором. Загалом використовують три фактори автентифікації: “те, що я знаю” (наприклад, пароль), “те, що я маю” (наприклад, картка, токен) та “те, що мене характеризує” (біометрика). Автентифікація застосовується в системах контролю і управління доступом із використанням одно- або двофакторної автентифікації.

Зазвичай стандарт 802.11 стосується комп'ютерної інформації. Сьогодні існує велика кількість пристроїв, якими керують з використанням радіоканалу, для яких проблема захисту даних є так само гострою. Наприклад, поширені системи автосигналізації, де використовується радіоканал. Для сучасних автобрелоків характерні недоліки: спрацювання незалежно від того, чи є поблизу інші пристрої, що працюють у тому самому діапазоні (що може викликати перекриття сигналів та створення взаємних завад), а також низький рівень захисту, який ґрунтується на однофакторній автентифікації (те, що власник має – брелок), як правило, зі статичними кодами авторизації. Заглядаючи наперед, можна припустити необхідність безпечного зв'язку користувача із власним автомобілем не тільки для блокування та розблокування дверей, але й для виконання інших функцій, наприклад, підтримки певного кліматичного режиму у салоні. Тому не варто обмежуватись тільки розглядом процедури автентифікації, – слід розглядати весь комплекс проблем AAA із подальшим шифруванням даних.

Ще одним прикладом є система за назвою “розумний будинок” (“розумний офіс”, “розумне місто”) [2]. У цих системах під безпекою об’єкта розуміють пожежну, антивандальну безпеку, безпеку від проникнення, але ніяк не безпеку доступу до функцій керування. Питання захисту конфіденційної інформації, яка може міститись у такому об’єкті, досі не розглядали. В системі “розумний будинок” одним з необхідних елементів безпеки керування на відстані стає взаємна автентифікація користувачів та серверу, що в принципі не передбачено в реалізації системи централізованого доступу RADIUS (Remote Access Dial-In User Service).

### Основна частина

Під дистанційним керуванням розумітимемо передавання автентифікаційних факторів бездротовим каналом передавання даних. У разі використання тільки гігагерцового діапазону небезпека, яка може виникати – перехоплення цієї інформації пристроями, аналогічними приймачу власника. Відома, наприклад, система перехоплення за назвою кодграбер (“code grabber”, “захоплювач коду”). Розрізняють три типи таких пристроїв: кодграбер для статичних кодів, кодграбери за принципом кодопідміни (для одно- и двокнопкових брелоків) та алгоритмічні (інколи їх називають “мануфактурними”, або кодами виробника) [2].

Використання статичних кодів є небажаним через те, що такий код достатньо легко можна перехопити кодграбером і використати замість брелока.

Для кодграберів, заснованих на принципі кодопідміни, характерним є такий алгоритм роботи, що вимагає повторного натискання власником кнопок брелока. Кодграбер при цьому використовує одночасно радіоглушення і перехоплення посилки брелока. Матеріали за цією тематикою розташовуються у відкритому доступі на тематичних інтернет-ресурсах.

За третім варіантом використовується протокол “запит – відповідь”. Алгоритмічний кодграбер – пристрій, який розпізнає за цифровим посиланням брелока тип (тобто виробника, “бренд”) сигналізації і, використовуючи так званий “мануфактурний код”, стає клоном (повним дублікатом) брелока власника [3]. Цей принцип застосовується до автосигналізації, що використовує алгоритм Keeloq для кодування сигналу від брелока до центрального блоку сигналізації під час радіообміну “брелок – центральний блок” (діалогові системи). Вважається, що мануфактурні коди (“коди виробника”) для більшості типів сигналізацій отримано методами промислового шпигунства на заводах, що програмують мікроконтролери систем автосигналізацій, або в результаті зворотнього інженерного розроблення чипів мікроконтролерів. Існують “чорні списки” автосигналізацій, які розкриваються алгоритмічним кодграбером. Такий кодграбер, залежно від функцій і кількості “прошитих” автосигналізацій, коштує кілька тисяч доларів і використовується для тестування сигналізацій в автосервісах і страхових компаніях.

Протокол “запит – відповідь” ґрунтується на застосуванні мануфактурного коду, який надає деякий рівень безпеки. Цей протокол за своїх переваг потребує синхронної роботи системи та брелока. Кожний наступний запит дає новий код, який пов’язаний з попереднім. Синхронізація може здійснюватись за подією. Відповідь, яка надходить на запит від брелока, і код, що формується в системі, мають бути однаковими. За розсинхронізації може виникнути ситуація, коли вони не збігаються. Наприклад, під час натискання кнопки брелока вона може випадково спрацювати кілька разів, що призведе до розсинхронізації брелока і системи.

Для уникнення такої ситуації розглянемо детальніше протокол “запит – відповідь”. Брелок посилає кодове посилання, яке сприймає система. Система перевіряє (ідентифікує) брелок і визначає, що це той самий брелок, яким було закрито машину. Тут можна використати один з нескладних криптографічних алгоритмів, наприклад, потокове шифрування. Є номер брелока, який у зашифрованому вигляді подається на систему. Процедура потокового шифрування передбачає знання системою послідовності гами. Після ідентифікації система генерує запит і одночасно визначає код запиту та надсилає його брелоку. Брелок відпрацьовує запит і формує код відповіді, основуючись на знанні гами. Зворотним каналом код передається в систему, де порівнюється зі сформованим за такою самою процедурою кодом. У разі збігу спрацьовує виконавчий пристрій. Важливо, щоб під час обміну інформацією не було повторного спрацювання. Це може бути

Використання динамічної генерації коду посилює захист, але не дає змоги повністю запобігти зламу сигналізації. Додаткове дослідження показало, що для зламу 64 бітного ключа автомобільної сигналізації, що використовує мікросхему KeeLoq, потрібна приблизно година часу. Така ситуація виникає внаслідок недосконалого криптографічного захисту, тому що насправді динамічними є 28 бітів ключової послідовності, а решта 36 бітів являють собою мануфактурний код, який можна визначити для кожної марки автомобіля. Очевидно, що проблема полягає у недостатній стійкості ключа.

[illegible]

Брелок відсилає повідомлення А в систему сигналізації об'єкта. Система сигналізації порівнює повідомлення, що надійшло, з таким, що є в пам'яті – А1. Якщо А і А1 ідентичні, система ідентифікує брелок і надсилає повідомлення В1 брелку. Тим самим вона підтверджує успішну

ідентифікацію брелка. Одночасно система переходить у стан С1 і видає сигнал на виконавчий механізм для розблокування дверей. Тобто вона готова до наступного сеансу. Брелок отримує повідомлення В1, порівнює його з тим В, що є у пам'яті. Якщо В та В1 однакові, брелок ідентифікує систему та переходить у стан С. Він готовий до наступного сеансу.

У випадку, коли А не збігається з А1 (у випадку чужого об'єкта або чужого брелока), система не реагує на повідомлення, залишаючись у попередньому стані. Одночасно брелок не отримує повідомлення В1 і так саме залишається у попередньому стані.

Наведемо деякі оцінки. Для ключа в 64 біти кількість вмикань (натискань на кнопку брелока) до повного вичерпання гами становитиме орієнтовно 4000 для довжини псевдовипадкової послідовності  $2^{32}$  [4]. Ця кількість перемикачів забезпечує тривалість роботи системи на одному періоді гами протягом близько року. Тому аналіз коду з використанням кодграбера потребує достатньо значного часу.

Додатковим засобом забезпечення безпеки коду може бути застосування радіосигналу, що передається в межах егерцового діапазону, в якому записано ехо-сигнал, модульований контрольною інформацією. Цей сигнал надсилається на початку разом з повідомленням А, розшифровується системою, і у випадку збігу з деякою записаною в системі контрольною інформацією ініціюється робота протокола з використанням каналу зворотного зв'язку.

Треба зауважити, що стеганографічний захист інформації з використанням ехо-методу є достатньо критичним до спотворень сигналу, зокрема внаслідок впливу завад. Це обумовлено намаганням розробників зменшити часовий зсув ехо-сигналу для підвищення стійкості стеганографічного алгоритму. Відношення сигнал/шум залежить від відстані між джерелом і приймачем радіосигналу обернено пропорційно квадрату відстані. Визначити максимальну відстань

$r_{max}$  можна за співвідношенням:

$$r_{max} \sim \sqrt{I_0 / I_{ш}}.$$

Потужність сигналу брелока  $I_0$  обмежена ємністю батарейки живлення, а потужність завад  $I_{ш}$  вважаємо не залежною від відстані, і тому рекомендована відстань спрацювання 10–15 метрів. За таких умов уявляється реальним застосування ехо-методу для автентифікації брелока.

### Висновок

Проаналізовано сучасний стан систем сигналізації з дистанційним бездротовим керуванням. Виявлено принципові недоліки існуючих систем та використовуваних протоколів автентифікації.

Запропоновано посилений протокол автентифікації в системі зі зворотним каналом зв'язку, який по суті являє собою протокол взаємної автентифікації. Пропонується використовувати гаму псевдовипадкової послідовності, поділену на однакові частини по 64 біти.

Для додаткового захисту можна застосувати метод ехо-сигналів для передавання контрольної динамічної ідентифікуючої інформації.

1. Стандарт 802.11/ – [Електронний ресурс]. – Режим доступу: <http://ea-banks.ucoz.ru/load3-1-0-3>. 2. KeeLoq и дежавю – [Електронний ресурс]. – Режим доступу: <http://old.computerra.ru/offline/2007/700/331416/>. 3. Микросхемы KeeLoq с технологией “прыгающего кода” – [Електронний ресурс]. – Режим доступу: <http://www.microchip.ru/files/d-sheets-rus/keeloq.pdf>. 4. Нємкова О. А., Шандра З. А., Ганій С. С. Застосування луна-сигналів для автентифікації звукових файлів – [Електронний ресурс]. – Режим доступу: [http://www.businessstudio.ru/buy/modelshop/nm\\_bank2](http://www.businessstudio.ru/buy/modelshop/nm_bank2).