Протокол для забезпечення інформаційної безпеки в системі "Розумний будинок"

Олексій Ляшенко, Денис Гольцев

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

In this paper, we propose an implementation option for a protocol for secure data exchange between smart home network devices. The models necessary to solve the problem of ensuring secure interaction using low-resource cryptography in a smart home network are considered. A software implementation of the proposed protocol was developed using the example of a smart home network.

Ключові слова – розумний будинок, протокол інформаційна безпека, моделі загроз.

I. Вступ

В рамках даної роботи загальна проблема безпеки Інтернету речей була зведена до окремого випадку - безпеки пристроїв розумного будинку. Метою даної роботи є забезпечення безпеки взаємодії між компонентами середовища розумного будинку. Розумний будинок, як підмножина елементів Інтернету речей в роботі визначено у вигляді набору пристроїв, пов'язаних в єдину мережу, метою якої є автоматизація всіляких побутових процесів [1]. У загальному випадку розумний будинок не є повністю автономної мережею - користувач має можливість втручатися в роботу пристроїв, здійснюючи безпосереднє керівництво. В даний момент на ринку представлені такі методи управління агентами розумного будинку [2]:

− автоматизоване, рішення приймається на основі інформації з датчиків;

− за допомогою централізованої панелі управління (всі пристрої - одна панель управління);

− за допомогою пульта (один пристрій - один пульт);

− комбінований.

II. Модель фізичного середовища

Для створення протоколу, що забезпечує належний рівень безпеки взаємодії в рамках мережі, при цьому не навантажує згадану мережу зайвим функціоналом, необхідно сформувати правильне розуміння середовища функціонування і загроз функціонуванню. Таким чином, необхідно сформувати моделі, що забезпечує як адекватне сприйняття фізичної і віртуальної середовища, так і дозволяють зрозуміти, що саме здатне порушити функціонування системи в згаданих середовищах.

Розглянемо поняття фізичної середовища з точки зору пристроїв розумного будинку. Під фізичним середовищем мається на увазі пряме оточення пристроїв, здатних на взаємодію з ним. Модель фізичного середовища, з точки зору безпеки, не відповідає на питання про адекватність застосування агента в тому чи іншому середовищі. При цьому модель оточення повинна враховувати середу поширення сигналу (як джерело загрози) і користувача (авторизованого, як джерела команд і неавторизованого, як джерело загрози). Слід зазначити, що незважаючи на те, що з точки зору розробляється протоколу не існує жодних методів вплинути на загрози з фізичної середовища, модель згаданого середовища необхідна для розуміння особливостей розробки в сфері розумного будинку і налаштування обладнання. Застосування інтерфейсів авторизації, електронних ключів і інструментів біометрії дозволяє істотно знизити ризики, пов'язані із взаємодією на фізичному рівні. Крім того, неадекватне сприйняття фізичної середовища здатне привести до неправильного функціонування обладнання.

Слід зазначити, що взаємодія на фізичному рівні, це коли порушник має прямий доступ до агентам мережі. Дана модель перетинається з моделлю загроз у сфері порушень, пов'язаних з доступом до середовища поширення інформації.

III. Модель експериментальної системи

Для створення повноцінної моделі експериментальної середовища, необхідно визначити кожен з об'єктів згаданого середовища.

Для спрощення сприйняття моделі визначимо поняття часу виконання операції, у вигляді тимчасового проміжку t між надходженням запиту (із зовнішнього середовища або при виконанні коду на обчислювальній машині). Тоді під адекватним часом виконання операції буде матися на увазі відрізок $t < delta\ t$, де $delta\ t$ - час між останнім запитом на виконання операції і новим запитом на виконання операції. Поняття адекватного часу виконання критично важливо для розуміння можливості впровадження додаткових заходів захисту.

Визначимо базовий контролер у вигляді обчислювальної машини, здатної виробляти складні, з точки зору протоколу, операції за адекватний час. Так як розроблений протокол не має сенсу поза фізичного носія (мережі розумного будинку), наділимо базовий контролер можливістю створювати згадану мережу. Тоді, саме базовий контролер відповідає за реєстрацію нових агентів мережі, зберігання інформації про агентів і передачу інформації в шлюз або на пристрій обробки інформації. Крім того, базовий контролер відповідає за виконання функцій безпеки. З точки зору ієрархії системи знаходиться на першому рівні маючи доступ до другого рівня.

Також була розроблена модель, яка необхідна для розробки протоколу в рамках даної роботи, це модель загроз, спираючись на яку можна судити про адекватність застосування тих чи інших рішень безпеки в протоколі.

Основним завданням даної моделі є визначення кінцевого числа загроз, які несуть найбільший ризик з точки зору протоколу взаємодії в мережі, для подальшого пошуку рішень по мінімізації згаданих ризиків від кожної конкретної загрози. В якості зовнішньою загрози розглядаємо загрозу, джерело якої знаходиться за межами мережі і потенційно має доступ до неї через шлюз. Наявність в моделі зовнішніх загроз виправдовує необхідність застосування заходів захисту до шлюзу. Внутрішньою загрозою назвемо загрозу, джерело якої знаходиться всередині мережі.

Слід зазначити, що в подібному вигляді модель є надмірною. Робота з реальної експериментальним середовищем показала неадекватність проведення атак, пов'язаних з підробленими агентами в рамках даних в цій роботі визначень. На Рис. 1 запропонована схема експериментальної системи – носія розробленого протоколу.

Аналогічно можна виключити компрометацію агента - порушення подібного рівня має на увазі прямий доступ до агенту на фізичному рівні та запобігає застосуванням технічних, а не програмних засобів. При цьому застосування подібних середовищ вимагає наявності обчислювальних потужностей до агента, що, з точки зору моделі, перетворює його в зовнішній контролер.

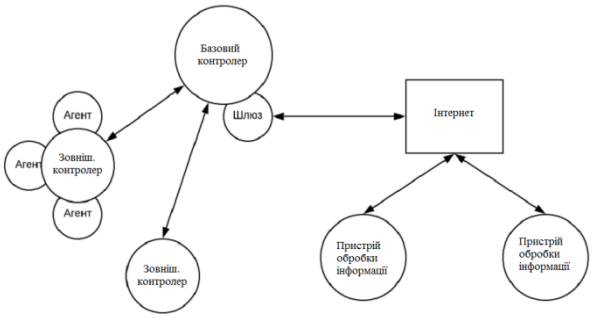

Рисунок 1 – Схема експериментальної системи

IV. Структура базового пакета протоколу

Розглянувши обмеження, що накладаються реалізацією стека протоколів передачі даних, можна зробить висновок, що з будівлі фрейму, що базове обмеження на розмір пакета в реалізованому протоколі становить 2313 біт. Дане обмеження не є критичним, так як підсумковий пакет протоколу залишає істотний запас для передачі. Для надійного механізму підтвердження, необхідно ввести поля флагів і заголовків, для спрощення ідентифікації пакетів і прискорення їх обробки [2].

Так як мова йде про обмін інформацією всередині мережі розумного будинку, необхідність додаткової кодування відсутня - завдання обробки даних лягає на кінцевого адресата даних. Вид отриманого розробленого пакету представлений на Рис.2.

Заголовок	Flag	Дані	Контр. число	Метки
8	8	0 - 263	16	16

Рисунок 2 – Базове представлення пакета

Заголовок включає в себе наступні біти: K - зазначає повідомлення як частина процедури зміни ключа; N - зазначає повідомлення, як частина процедури установки нового пристрою; D - зазначає повідомлення, як частина стандартного обміну даними; M - зазначає повідомлення, як частина процедури вирівнювання міток; BR - зазначає повідомлення, як передачу, яка транслюється на всю доступну підмережа (не скасовує ієрархічні обмеження на обмін даними); B - зазначає повідомлення, як повідомлення від базового контролера; E - зазначає повідомлення, як повідомлення від зовнішнього контролера; A - зазначає повідомлення, як відправлене агентом.

Поле контрольного числа відповідає за підтвердження успішної пересилання. Застосовується спільно з бітами W і E поля прапорів.

Являє собою пару пару $(x, F(x))$, де x - випадкове число, що генерується відправником, а $f(x) = x + Int(add8)\ mod\ 2\ ^\wedge\ 16$ - відповідь. Тут $add8$ - перші 8 інформаційних біт. У разі задіяного прапора C поле даних підлягає розшифруванню перед обробкою.

Висновки

При необхідністі застосування механізмів безпеки всередині мереж розумного будинку, мала потужність елементів подібних мереж накладає істотні обмеження на можливі механізми безпеки. Алгоритми, ефективні на великих масивах даних, при використанні на серверах і персональних комп'ютерах, часто непридатні в умовах відсутності запасу пам'яті і процесорного часу. Таким чином, необхідно застосування більш економічних алгоритмів. Ефективне функціонування мережі досягається так само за рахунок мінімізації витрат на пересилку окремого пакета шляхом скорочення його полів і розміру. При розробці протоколу для мережі, що функціонує на обладнанні малої обчислювальної потужності, необхідно також враховувати особливості обладнання, умови, в яких воно функціонує і призначення подібного обладнання. Так, протокол, оптимальний для мережі розумного будинку буде непридатний для промислового інтернету речей. При виборі криптографічних алгоритмів, що застосовуються в рамках мережі обладнання малої потужності, важливим критерієм є не тільки криптографічний стійкість і обчислювальна простота, а й наявність стандартів застосування даного алгоритму.

Література

[1] Liashenko O. Model of the work of the neurocontroller to control fuzzy data from the sensors of the climate control subsystem “smart house”. / O. Liashenko, O. Barkovska, C. Al-Atroshi, O. Datsok, S. Liashenko // International Journal of Advanced Trends in Computer Science and Engineering, 2019. – №8(1), C. 70-74.

[2] Wenling Wu. LBlock: A Lightweight Block Cipher. / Wu Wenling, Zhang Lei // International Conference on Applied Cryptography and Network Security ACNS 2011: Applied Cryptography and Network Security P. 327-344