ЗАХИЩЕНИЙ КАНАЛ ЗВ'ЯЗКУ КОНЦЕПЦІЇ «РОЗУМНИЙ БУДИНОК»

Туріцин М. В.
(Науковий керівник Євграфов Д. В., к.т.н., доцент)
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Радіотехнічний факультет

При управлінні системою «розумний будинок» використовується відкрита мережа Інтернет. Тому актуальною задачею являється створення захищеного каналу зв'язку для безпечного управління такою системою. При проектуванні "розумного будинку" інженери впроваджують різноманітний функціонал. В табл. 1 приведено список основних напрямків функціоналу системи "розумний будинок" та ступені небезпеки при доступі зловмисника до функціоналу, де перша ступінь – легка, четверта – найважча.

Таблиця 1. Основний функціонал системи "розумний будинок"

Степінь небезпеки при несанкціонованому доступі зловмисника до системи	Назва системи
II	Система електричного живлення та освітлення
I	Мультимедійна система
IV	Охоронна система та система дистанційного управління
III	Система контролю клімату та обслуговування території

З таблиці можна помітити що найгіршим наслідком при несанкціонованому доступі є управління системою охорони через систему дистанційного керування. Так зловмисник спокійно зможе проникнути в будинок і виконати будь-які дії. Також може спричинити пожежу, потоп та інші дії, використовуючи доступний функціонал системи дистанційно.

При дистанційному управлінні системою використовується відкрита мережа Інтернет. Тому зловмисник, використовуючи спеціалізоване програмне забезпечення, може отримати доступ до пункту керування системою "розумний будинок".

Для запобігання несанкціонованого доступу необхідно створити безпечне з'єднання системи "розумний будинок". Це можна зробити різними способами. Оптимальний спосіб це створення мережевого тунелю.

Було проведено створення такого тунелю на мові програмування PHP. В основі створення захищеного тунелю лежить алгоритм шифрування RSA-1024. Учасники обміну інформації з'єднуються з мережею Інтернет не на пряму, а через сервери-посередники. Сервери-посередники ж створюють захищений канал зв'язку через відкритий доступ Інтернету.

Частина тестового коду програми приведено в табл. 2.

Таблиця 2. Код програми

Код програми

```
<?php
$p = 11;
$q = 12;
$n = $p * $q;
$fi = ($p - 1) * ($q — 1);
$i = 1;
while (($d = ($i * $fi + 1)) % $e !== 0) {
   $i++;
}
$d = $d / $e;
$sym =8;
$encryptSym = pow($sym,$e)%$n;
$encrypt_exponent_d = $encryptSym;
for ($i = 1; $i <$d; $i++) {
$encrypt_exponent_d = ($encrypt_exponent_d * $encryptSym)%$n;
}
echo "$encrypt_exponent_d <br />";
$decryptSym = $encrypt_exponent_d%$n;
$outSym = chr($decryptSym);
```

Таким чином власник системи “розумний будинок”, назвемо його учасник “А”, звертається до системи, але насправді з’єднання відбувається з сервером-посередником, а вже сам сервер встановлює з’єднання з системою. Це все відбувається прозоро. Таким чином ні учасник ”А” ні сама система не здогадуються про сервер посередник.

Згідно отриманих результатів захищений канал зв’язку суттєво зменшує шанси отримання контролю над системою “розумний будинок”. А саме, для розшифрування ключа необхідно витратити 95 років процесорного часу, за умовою участі кілька сотень комп’ютерів. Для отримання доступу до системи “розумний будинок” без захищеного каналу буде достатньо години.

Література

1. Можливості системи “розумний будинок”. [Електронний ресурс]. Доступно за посиланням: https://smart-home.market/vozmozhnosti-umnogo-doma-obzor-sistem-s3081 Останній вхід 15.04.2018.

2. 100 функцій системи “розумний будинок”. [Електронний ресурс]. Доступно за посиланням: http://www.besmart.su/article/100_funkciy_udml Останній вхід 27.04.2018.

3. Проектування системи “розумний будинок”. [Електронний ресурс]. Доступно за посиланням: http://stroyka-gid.com.ua/instrykziy/13557-proektyvana-systemy-rozumny-bydynok.html Останній вхід 28.04.2018.

4. Документація по мові програмування PHP. [Електронний ресурс]. http://php.net/ Останній вхід 26.04.2018.

5. Скільки часу потрібно для щоб підібрати ключ шифрування в RSA. [Електронний ресурс]. https://security.stackexchange.com/questions/4518/how-to-estimate-the-time-needed-to-crack-rsa-encryption