4. Голев Д.В. Інформаційна безпека інформаційно – комунікаційних систем. Навч. Посібник / Г. Кононовича. / Д.В. Голев, О.Ю. Русляченко, Ю.В. Бєлова, Д.С. Гончарук – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 184 с.

Невмержицький В. В.,
Криворізький національний університет
Кузнєцов Д.І.,
к. т. н., доцент, Криворізький національний університет

ОХОРОННА СИГНАЛІЗАЦІЯ ТА КРИПТОСТІЙКІ АЛГОРИТМИ ЇЇ ШИФРУВАННЯ

Досліджено системи охоронної сигналізації, діапазони частот їх роботи. Проаналізовано різні алгоритми та способи захисту які наявні на ринку сигналізацій.

Охоронна сигналізація призначена для захисту житла чи автомобіля від несанкціонованого проникнення, і в даний час набула широкого поширення. Це кращий спосіб забезпечити охорону вашого майна під час вашої відсутності.

Бездротова система сигналізації має такі якості, як портативність, легкість у встановленні й відсутності зайвих дротів. Всі сигнали для зв'язку з пристроями передаються по жорстко заданим частотам. Як правило, в кожній країні є свій безкоштовний спектр радіочастот, а є урядовий, розподіл якого регулюється постановою «Про затвердження Національної таблиці розподілу смуг радіочастот України», від 15 грудня 2005 р. № 1208[1].

У документі перераховано весь перелік існуючих радіочастот і вказані в яких діапазонах дозволено використовувати комерційним організаціям. Згідно з додатком частота 433MHz лежить в діапазоні: 433,05 - 434,79 МГц і відноситься до неспеціалізованих пристроїв радіочастотної ідентифікації, пристроїв охоронної радіосигналізації автомашин, а частота 868MHz (868 - 870 МГц) до неспеціалізованих пристроїв охоронної сигналізації. На базі цих частот створюють бездротові охоронні сигналізації.

До безкоштовних бездротових каналів зв'язку відноситься міжнародний діапазон ISM. Для його застосування не потрібно ліцензування. Bluetooth, Wi-Fi, IEEE 802.15.4, Zigbee працюють в цьому діапазоні.

Завдяки високій швидкості роботи радіоканалу, високої стійкості до помилок зв'язку та малому енергоспоживанню цей діапазон застосовується в більшості сучасних пристроїв. Частоти 433MHz і 868MHz -— це дві головні групи, які зазвичай використовуються в системі бездротової сигналізації.

Дальність дії пристроїв, що працюють на частоті 433MHz і 868MHz невелика, і скорочується в залежності від наявності сторонніх об'єктів на шляху передачі сигналу. Частота 433MHz добре себе зарекомендувала для рухливих об'єктів. 868MHz має перевагу у швидкості передачі, обміну даних і дальності передачі сигналу.

Алгоритм шифрування в охоронних системах — набір правил обміну даними між пультом і блоком управління сигналізації, за якими здійснюється захист передачі даних, щоб зловмисник не зміг дістати несанкціонований доступ в автомобіль чи будівлю, навіть якщо зможе перехоплювати пакети обміну даними.

Алгоритми найперших сигналізацій ґрунтувалися на статичному кодуванні. При цьому була всього одна команда для однієї дії, ця команда була статичною та не змінювалась під час експлуатації. Наприклад, команді «закрити двері» завжди був код для надсилання «Z999X» (в такому форматі він передавався від пульта на блок управління). Тоді, коли варіантів коду сигналів було мало, то іноді своїм пультом можна було відчинити іншу машину з такою ж сигналізацією — формати кодів для управління збігалися. Таке кодування не могло забезпечувати належного захисту досить було один раз переловити код відповідної однієї із команд, а потім використовувати її для несанкціонованого доступу.

Зараз на ринку є стійкі до електронного злому системи, цим користуються виробники, які масово виробляють сигналізації. Є таке поняття — мануфактурний код. Фактично це статична база даних електронних посилок, якими обмінюються між собою пульт і сигналізація. Мануфактурні коди, якимсь чином, виявляються у розробників код-граберів і заносяться в пам'ять пристроїв. Після цього граберу досить перехопити одну з команд, щоб пристрій вирахував наступну команду і почав працювати, як штатний пульт. І, до речі,

саме сканування в цьому випадку відбувається непомітно для справжнього власника.

Не піддаються скануванню сигналізації з так званим діалоговим кодом, але, на жаль, часом його вписують в характеристики безпідставно, так би мовити, в маркетингових цілях. Тому, вибираючи сигналізацію, можна побачити в характеристиці Dialog Code а насправді такий код там не використовується. Сигналізаціями які зараз є стійкими до код-граберів являються: Pandora, Magnum, Magic Systems, Starline, Prizrak[2].

Діалоговий код — це не послідовність заздалегідь прописаних сигналів, а індивідуальний алгоритм обробки посилок, який робить перехоплення окремих кодів безглуздим.

Коли власник натискає на кнопку, з пульта на центральний блок сигналізації приходить запит на виконання команди. Далі блоку управління потрібно впевнитися в тому, що команда відправлена саме з пульта власника. Для цієї мети він генерує випадкове число і відправляє його на пульт. Це число за певним алгоритмом обробляється і передається назад на блок управління. В цей же час блок управління обробляє то саме число і порівнює його з числом надійшовшим від пульта. В тому і тільки тому випадку, якщо числа збігаються, центральний блок сигналізації виконує команду. Варто зазначити, що алгоритм, за яким виконуються розрахунки над випадковим числом, суто індивідуальний для кожної сигналізації, закладається в неї ще на етапі виробництва і в більшості випадків є комерційною таємницею.

ВИСНОВКИ

На сьогодні є досить багато охоронних сигналізацій як для автомобіля так і для будівель. Сучасні методи криптостійкого захисту можуть забезпечити максимальний захист, але зловмисники теж знаходять методи їх злому, тому всі системи охоронної сигналізації потребують постійного вдосконалення та розробки нових алгоритмів шифрування сигналу.

ЛІТЕРАТУРА

1. Про затвердження Національної таблиці розподілу смуг радіочастот України [Електронний ресурс].–Режим доступу https://zakon.rada.gov.ua/laws /show/1208-2005-п

2. Алгоритмический кодграббер и диалоговый код. [Електронний ресурс].–Режим доступу https://www.drive2.ru/b/1619320/

Дзензура А. А.,
Криворізький національний університет
Кумченко Ю. О.
к.т.н., доцент, Криворізький національний університет

ЗАХИЩЕНЕ ЛОКАЛЬНЕ МЕРЕЖЕВЕ СЕРЕДОВИЩЕ ДЛЯ ЗБЕРІГАННЯ ФАЙЛІВ НА ОСНОВІ NAS

Розглянуто основні види загроз та засоби захисту локального мережевого середовища на основі NAS. Запропоновано схему побудови захисту сервера та зображено типові методи атак.

Тема захисту інформації, загалом конфіденційних даних, є дуже важливою та актуальною у наш час. Власники інформаційних систем, які не надають належної уваги до захисту, ризикують витоком, знищенням та спотворенням важливої інформації.

Мережеве сховище знаходиться в стані захищеності, якщо забезпечена доступність, конфіденційність та цілісність інформації. Дані, які знаходяться в локальних (LAN), або в глобальній мережах (WAN), постійно піддаються різним видам загроз. Найбільш поширеними видами атак, на локальне мережеве середовище для зберігання файлів на основі Network Attached Storage (NAS), є наступні:

1) прослуховування мережі (Sniffing) – крадіжка або перехоплення даних шляхом захоплення мережевого трафіку за допомогою спеціалізованого ПЗ – Sniffer;
2) атака-вторгнення (Invasion Attack) – перехоплення управління ресурсами мережі;
3) відмова в обслуговуванні (Denial of Service) – атака на обчислювальну систему з метою довести її до відмови;
4) ping-флуд (Ping Flooding) – приведення сервера до відмови шляхом великої кількості запитів;