УДК 343.98

Г. В. Куцо
старший науковий співробітник

Одеський науково-дослідний інститут судових експертиз
Міністерства юстиції України

ДОСЛІДЖЕННЯ АЛГОРИТМІЧНОГО КОДГРАББЕРА

У статті розглянуті питання проведення досліджень високотехнологічного обладнання, зокрема, алгоритмічного кодграбберу.

На даний час спостерігається стрімке збільшення кількості злочинів, пов'язаних з крадіжками особливого майна з транспортних засобів або неправомірним заволодінням транспортними засобами. В деяких з випадків правопорушники використовують високотехнологічне обладнання — кодграббери. З метою приховування своїх дій правопорушники використовують кодграббери, доступ до яких захищено паролем, а спосіб управління режимами роботи кодграббера не є відомим експертам.

Актуальність цієї статті пов'язана з тим, що в системі Міністерства юстиції України, Міністерства внутрішніх справ України, Служби безпеки України поки відсутня методика проведення досліджень цих пристроїв. В більшості випадків розслідування злочинів, при яких використовувались кодграббери, проводяться без експертного супроводу або експертний супровід надає негативні висновки.

Складність розробки методики пов'язана з постійним оновленням програмного забезпечення кодграбберів, їх видової різноманітності, потреби розробки спеціалізованого обладнання.

Поняття кодграббер, історія створення кодграбберів

Кодграббер — пристрій, призначений для несанкціонованого втручання в роботу автомобільної сигналізації шляхом перехвату та обробки сигналу з пульта автомобільної сигналізації автовласника, що надає можливість отримання повного доступу до охоронної сигналізації автомобіля.

Перші офіційні згадування про кодграббер можна зустріти в статті «Брелок за сто тысяч» 11-го випуску за 2008 рік журналу «За кермом».

Системи перехоплення та обробки сигналу з пульта автомобільної сигналізації можливо поділити на три групи:

- сканери (для охоронних систем зі статичним кодом, які вироблялись до середини 90-х років).

- кодграббери (для охоронних систем з плаваючим кодом, які почали вироблятися з 1995 року). Алгоритм плаваючого коду було розроблено компанією «Microchip», отримав назву «KeyLoq» та передбачав передачу окрім статичної частини — динамічної частини, що формувалось за певним алгоритмом. Код цього виду має наступну структуру:

- 4 байти динамічної частини;

- 4 байти статичної частини (серійний номер пульта);

- 2 байти з кодом натиснутої на пульті кнопки.

Цей код повторюється із заданим інтервалом, поки утримується кнопка. Друга посилка записується у пам'яті кодграбберу і може використовуватись для зняття з охоронної сигналізації.

Алгоритмічний кодграббер (для охоронних систем з плаваючим кодом на базі мануфактурного коду (ключ шифрування)). Алгоритмічні кодграббери з'явились у 2005 році і призначені для повного відтворення пульта автовласника.

Для того, щоб отримати мануфактурний код, необхідно зчитати прошивку (програму) з мікропроцесора пульта. Це досить тривалий та складний процес. Кожен з виробників автосигналізацій з мануфактурним кодом блокує можливість зчитування прошивки. Принцип роботи алгоритмічного кодграббера:

- перехоплення посилки від пульту автовласника;
- вилучення серійного номеру пульта і запис у пам'ять алгоритмічного кодграбберу;
- визначення за серійним номером виробника охоронної автосигналізації;
- отримання функцій пульта автовласника за визначеним мануфактурним кодом виробника.

Як правило, алгоритмічні кодграббери не глушать сигнал оригінального пульта, тому його робота залишається непомітною для автовласника. Останні покоління алгоритмічних кодграбберів мають додаткові функції, такі як доступ до пристрою за пін-кодом, пам'ять на кілька пультів, їх додавання, видалення, блокування зворотного зв'язку тощо.

Для боротьби з алгоритмічними кодграбберами виробники охоронних систем реалізують в своїх продуктах «діалоговий код», тобто двосторонній обмін даними між пультом і сигналізацією за принципом інтерактивної авторизації.

В цій статті наводиться приклад дослідження алгоритмічного кодграббера на базі пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» [1], що використовується при скануванні автосигналізацій з діалоговим кодом.

Принцип дії кодграбберу заснований на перехопленні першої посилки (частотно-модульований радіосигнал) та збереження динамічної частини першої посилки (4 байти), після чого остання частина першої посилки та динамічна посилка наступної частини глушаться (білий шум). Далі обробляється наступна частина другої посилки — запам'ятовується статична частина (4 байти) та код натисненої кнопки (2 байти), остання частина глушиться. Глушаться і наступні посилки, які містять однакові динамічні частини сигналу. Ці дії надають можливість отримання повного коду, його збереження в пам'яті кодграбберу, блокування роботи пульта основного блоку автомобільної сигналізації автовласника. За результатами роботи кодграбберу автовласник не в змозі управляти автосигналізацією, і, як наслідок, ще раз (як міні-

мум) натискає кнопку пульта. У цей момент кодграббер повторює попередні операції з перехоплення і глушіння посилки, після чого відправляє в ефір посилку, записану при першому натисканні кнопки на пульті.

Приклади питань до вирішення судової експертизи алгоритмічних кодграбберів:

1. Чи відповідає наданий на експертизу пристрій своїм функціональним призначенням — пульта автомобільної сигналізації «(назва моделі)»?

2. Чи придатний наданий на дослідження пристрій для використання в якості пульта управління автомобільної сигналізації автомобілю «(модель автомобіля)», державний номер (державний номер)?

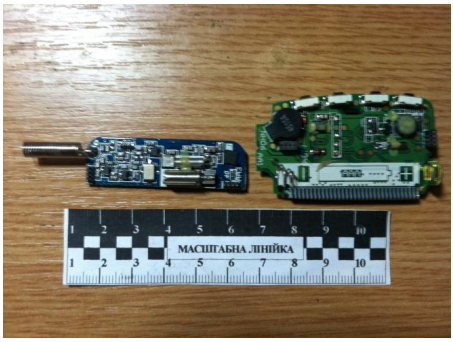
3. Чи може наданий пристрій використовуватися для сканування інформації автомобільної сигналізації автомобілю «модель автомобіля», державний номер (державний номер) (сигнал відключення і включення)? Якщо так, то яким чином?

4. Чи збережена інформація про коди автомобільних сигналізацій в пристрої, наданому на дослідження? Якщо так, чи присутня серед збереженої інформації — коди відключення і включення автомобільної сигналізації, що встановлена в автомобілі «модель автомобіля», державний номер (державний номер)?

Складова частина кодграббера

Кодграббери виготовляються на базі пультів автомобільної сигналізації, в якій присутні дві плати – плата управління та плата радіо-модуля:

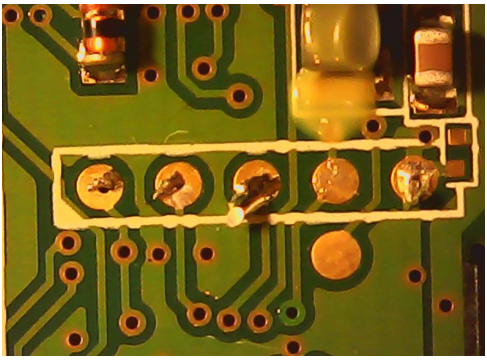
Зображення 1



Зображення 2

Плата управління містить основні елементи: рідкокристалічний екран (у подальшому РКЕ), мікроконтролер. Плата радіо-модуля містить основні елементи – антена, передавач радіохвиль, приймач радіохвиль, вібраційний елемент.

На електронній платі управління присутні чотири контрольні контакти друкованої плати, які надають можливість отримання доступу до перепрограмування мікроконтролера:



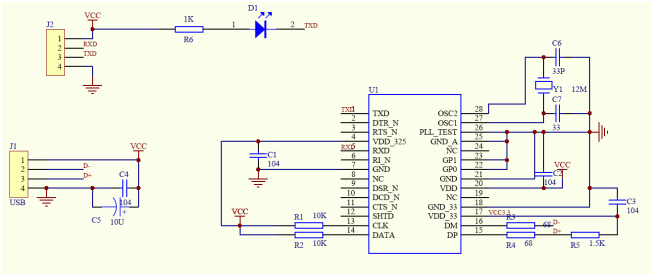
Зображення 3

При кустарному перепрограмуванні ці контакті можуть мати сліди підключення (залишки припою). При проведенні судових експертиз ці залишки припою надають можливість припустити, що було проведено перепрограмування шляхом припаювання до токопровідних контактів друкованої плати електричних проводів, які були під'єднанні до контролер-програматору.

Як приклад можливо навести контролер-програматор типу USB RS232 TTL PL2303HX [2]:

Зображення 4

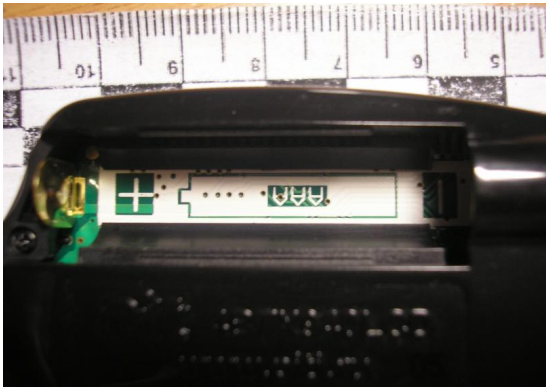
що побудовано на базі мікроконтролеру PL2303HX. Типова схема включення:



Зображення 5

Програматор використовується як перехід з UART (COM) с рівнями TTL-логіки (0-5 вольт) — послідовний інтерфейс з рівнем напруги 0-5 вольт. Для використання програматора у складі комп'ютера з операційною системою (в подальшому ОС) Micrisoft Windows потрібні драйвери від компанії виробни-ка (PL-2303 USB to Serial Bridge Controller) [3]. При роботі з програматором може використовуватися будь яка термінальна програма, як приклад – «HiperTerminal».

У складі пультів автомобільної сигналізації (кодграбберів) використовується елемент живлення типу «ААА», робочою напругою 1,5 вольт:



Зображення 6

Зовнішні ознаки відміни оригінального пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» сигналізації від кодграбберу.

При включенні оригінального пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» повинно відбуватись завантаження оригінального програмного забезпечення виробника цього типу автомобільної сигналізації, що супроводжується музичною фонограмою та відображенням на екрані всіх можливих позначок режимів роботи:

Зображення 7

Особливістю роботи програмного забезпечення кодграбберу на базі пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» є відсутність при включенні (підключення елементу живлення до пульта) програвання музичної фонограми, висвітлення на екрані всіх можливих позначок режимів роботи. При завантаженні програмного забезпечення кодграбберу на рідкокристалевому екрані присутнє лише одне позначення включеного режиму антипограбування (Anti-Hi-Jack):

Зображення 8

За складовою частиною (печатна плата, склад електронних компонентів, корпусу) кодграббер не відрізняється від стандартного пульта автомобільної сигналізації «Sheriff ZX-1095 PRO».

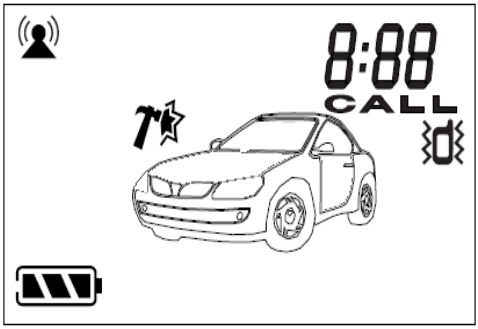
Активація роботи кодграбберу на базі пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» та основні позначення на рідкокристалевому екрані

З метою зручності подальшого опису, кнопки управління кодграбберу було умовно пронумеровано. Так, кнопку постановки на сигналізацію у подальшому позначено як кнопка «1», кнопку зняття з сигналізації - кнопка «2», кнопку вибору каналу - кнопка «3», кнопку функціональних можливостей - кнопка «4»:

Зображення 9

При підключенні кодграбберу до елементу живлення на РКЕ висвітлюється показник включеного режиму антипограбування (Anti-Hi-Jack). Інших робочих зображень немає.

Кодграббер на базі автомобільної сигналізації «Sheriff ZX-1095 PRO» може висвітлювати робочі зображення на РКЕ:



Зображення 10

Ці зображення режимів роботи визначають функціональні можливості:

Таблиця 1

	Йде сканування ефіру
	Йде передача сигналу
	Працює блокування зворотного зв'язку
	Отриманий сигнал розшифровано
	Номер осередку пам'яті.
	Отримано сигнал зворотного зв'язку від автомобіля
	Дистанційне відключення сирени в режимі «ОХОРОНА» (нічний режим)

Функціональні властивості управління кнопками №№1-4 наступні:

- кнопка 1: коротке натискання - постановки системи на охорону; довге натискання - автозапуск двигуна;
- кнопка 2: коротке натискання - зняття системи з охорони; довге натискання – синхронізація;
- кнопка 3: коротке натискання - перемикання комірки пам'яті; довге натискання - стерти елемент пам'яті;
- кнопка 4: коротке натискання - підсвічування дисплею; довге натискання - включення / виключення пристрою.

Короткі натискання кнопок дублюються одним звуковим сигналом.

При натисканні кнопки «4» у кодграббері активуються кнопки управління, що дублюється одним звуковим сигналом.

Побудований на базі автомобільної сигналізації «Sheriff ZX-1095 PRO» кодграббер може вмикатись у робочий режим тільки після введення вірного пін-коду[14]. Користувачем введення пін-коду виконується при натисканні на кнопки «1» та «2». При цьому кнопки «1» та «2» використовуються почергово наступним чином: кількістю натискань на кнопку «1» задається перша цифра пін-коду, друга цифра задається кількістю натискань на кнопку «2».

При успішному введенні пін-коду на рідкокристалевому екрані повинно висвітитися позначення:

Таблиця 2

	Йде сканування ефіру
	Отриманий сигнал розшифровано
1	Номер осередку пам’яті.
	Дистанційне відключення сирени в режимі «ОХОРОНА» (нічний режим)

Дійсно, при активованому режимі кодграбберу (введенні пін-коду) на РКЕ висвітлюються позначення:

Зображення 11

Для визначення пін-коду може використовуватись метод «Brute Force» (підбір паролю перебором) або цей код буде надано ініціатором проведення експертизи.

При проведенні експертизи фахівцю необхідно перевірити наявність збережених кодів автомобільної сигналізації по комірках пам’яті шляхом натискання на кнопку №3.

[14] PIN-код (англ. персональний ідентифікаційний номер - особистий розпізнавальний номер) - аналог пароля.

Так, наприклад, на Ілюстрації №10 показано, що в комірці пам'яті «2» кодграбберу було виявлено збережену інформацію раніше сканованого коду автомобільної сигналізації :

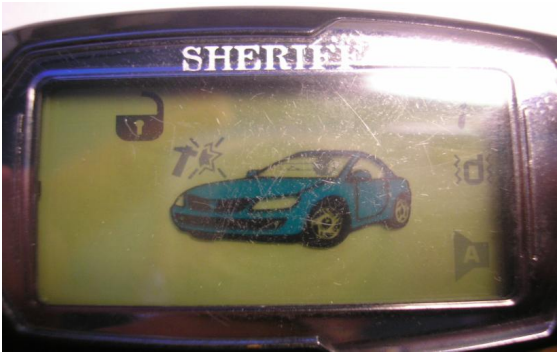
Зображення 12

Експериментальне дослідження роботи кодграбберу

Для встановлення факту функціонування кодграбберу необхідно проводити дослідження за використанням автомобілю потерпілого.

Експертом проводиться пробне сканування за допомогою кодграбберу автосигналізації автомобілю шляхом натискання кнопки відкриття дверей на пульті автовласника. При пробному скануванні на кодграббері обирається вільна комірка пам'яті (яка не має збережених кодів). Слід відзначити, що для чистоти експерименту потрібно обрати місце, віддалене від скупчення автомобілів. Це надасть можливість отримати лише код автосигналізації автомобіля, наданого на експертизу для проведення експерименту.

У разі успішного сканування в кодграббері спрацює вібраційний елемент, на РКЕ з'являться позначення «Отриманий сигнал розшифровано», «Комірка пам'яті 1», «Дистанційне відключення сирени в режимі «ОХОРОНА» (нічний режим)», «Блокування зворотного зв'язку», «Зняття з охорони».



Зображення 13

Після отримання кодграббером коду автомобільної сигналізації наданого автомобіля експертом проводяться поодинокі натискання кнопки «1» та «2» на кодграббері, завдяки чому отримується можливість постановки на сигналізацію та зняття з сигналізації наданого автомобіля .

Робота програмного забезпечення кодграббера на базі автомобільної сигналізації «Sheriff ZX-1095 PRO» визначає можливість постановки на сигналізацію та зняття з сигналізації наданого автомобіля в режимі «Працює блокування зворотного зв'язку».

Зображення 14

При використанні режиму «Працює блокування зворотного зв'язку» блокується зворотній сигнал роботи автомобільної сигналізації (на двосторонній пульт автосигналізації не надходять повідомлення про дії центрального блоку автосигналізації). Це є блокуванням інформації, яка передається з центрального блоку автомобільної сигналізації наданого автомобіля.

При проведенні експериментів необхідно перевірити всі раніше збережені коди автосигналізації на предмет наявності серед них кодів від автомобільної сигналізації потерпілого.

Крім того, рекомендується проведення експерименту з будь-якою іншою автомобільною сигналізацією модельного ряду, що підтримується цим кодграббером.

Побудовані на базі пульту автомобільної сигналізації «Sheriff ZX-1095 PRO» кодграббери мають можливість підбору кодів до управління наступних типів автомобільної сигналізації:

1). Sherif zx-999 (новий модельний ряд);
2). Sherif (модельний ряд keeloq) автозапуск;
3). Sherif (з новим динамічним кодом CFM моделі ZX-1055, ZX-1060);
4). Sheriff zx-9306;
5). Sheriff zx730 (з новим динамічним кодом CFM2) автозапуск;
6). Sheriff 750 CFM2 Новий ключ, нове шифрування;
7). Sheriff 940 CFM2 Новий ключ, нове шифрування;
8). Cool.Sheriff 1070 CFM2 Новий ключ, нове шифрування. Автозапуск.
9). Sher-Khan AM A (автозапуск), B, Vegas.
10). Sheriff 1090 CFM2 Новий ключ, нове шифрування. Автозапуск.
11). Sheriff T80-TOR T82-TOR.
12). Alligator S250,S275.
13). Alligator (з пейджерами зворотного зв'язку з новим кодуванням серії S-400 2WAY --- S-875 RS 2WAY)

14). Alligator (всі додаткові пульти keeloq)
15). Alligator (пейджери з жк дисплеєм, всі keeloq)
16). Alligator (пейджери зі світлодіодами, всі keeloq)
17). StarLine-Twage A6,A8,A9, автозапуск.
18). Cool.StarLine-Twage B6 (чорний брелок) автозапуск.
19). StarLine-Twage B6 (додатковий брелок) автозапуск.
20). StarLine-TwageB6 (синій пейджер) автозапуск.
21). StarLine-Twage B9 (чорний пейджер) автозапуск.
22). StarLine-Twage B9 (додатковий брелок).
23). StarLine 24V.
24). StarLine-Twage A4, A2 автозапуск.
25). StarLine-Twage B9 (діалоговий синій пейджер).
26). Pantera- (QX).
27). Pantera (SX).
28). Cool.Pantera (з пейджерами зворотного зв'язку до 5XXX серії).
29). Pandora (серія RX).
30). Pantera CLK 355.
31). Partisan
32). Pantera (SLK-350 SC-SLK-675 RS).33).APS 7000-9000.
34). APS 2700,2800,2900 Новий модельний ряд.
35). A.P.S. (увесь модельний ряд keeloq)
36). APS 2700,2800,2900 Новий модельний ряд.
37). Cenmax-MT7.
38). Cool. Cenmax (A-700 A-900).
39). Cenmax (VT-200, VT-210).
40). Cenmax (HIT-320 keeloq моделі).
41). CENMAX VIGILANT ST-5, ST-7, ST-10, V-7, MT-8 автозапуск.
42). Challenger (з новим динамічним кодом CFM2) автозапуск.
43). Challenger нові моделі зі зміненим кодом CFM моделі ch8000i, x-1.
44). Chelendger (увесь модельний ряд keeloq ch-7000i).
45). Mongouse.
46). Mangust EMS 1.7, 1.9, 1.7R, 1.9R автозапуск.
47). GUARD (брелоки з червоним світлодіодом keeloq).
48). Cool. Duplex.
49). Fighter.
50). Faraon.
51). KGB (додаткові брелоки, в тому числі старі моделі).
52). KGB (FX-3,FX-5, FX-7).
53). Berhut (додаткові брелоки).
54). Berkut (пейджери).
55). KGB (пейджери зі зворотним зв'язком типу VS 4000).
56). Godzila 4. Jaguar (увесь модельний ряд keeloq jx-2000).
57). Leopard.

58). Cool. Red Scorpio.
59). Inspektor.
60). FANTOM F-731, F-635LCD.
61). REEF (з червоним світлодіодом).
62). Gorgon (з червоним світлодіодом).
63). Black-Bug super (з червоним світлодіодом).
64). Fortress (частково).
65). Eaglemaster.
66). TIGER keeloq Tiger QS, Tiger MM1.
67). Partisan.
68). Cool. jaguar серія ja, jb.
69). Jaguar EZ-Betta, EZ-Alpfa, EZ-one.
70). Leopard LS нові моделі зі зміненим кодом, автозапуск.
71). Tomahawk X3 серія X автозапуск.
72). Tomahawk (TW7000), TW9000, TW9010, TW7010, TW7020, TW7030, TW9020, TW9030, 950LE) автозапуск.
73). Tomahawk TZ.
74). Top Guard.
75). Advanced.
76). Harpoon H1, H2.
77). AME-MM2 Type2 автозапуск.
78). Cool. Bagira MS AME-002.
79). DaVinci codeice 7k1,K9.1 автозапуск.
80). Convoy XS.
81). Black-Bug (зелений світлодіод).
82). Anaconda.
83). KLIFFORD 1998.
84). Mystery пейджери mx-605, mx-605RS, mx-705.
85). Mystery додаткові брелоки mx-605, mx-605RS, 607, 705, 905, 905RS.
86). Mystery пейджери mx-605, mx-605RS, 607, 705, 905, 905RS.
87). Mystery (пейджер зі світлодіодами) MX-503, MX-505.
88). Cool.KLIFFORD 1996.
89). SIRIO 777.
90). EXCALIBUR.
91). TAMPERS.
92). Reef (зелений світлодіод).
93). ZORRO.
94). OMEGA.
95). ENFORCER.
96). Visonic.
97). ROLLINS.
98). Cool. PRESTIGE.

99). Whister.
100). SKUNET.
101). Bagira bc-ame002.
102). Tiger EMS 1.7R, 1.9R.
103). CAYMAN C1.
104). Stinger-2000R.
105). MSRF-3k,MSRF-3D k-500k.
106). Magic Systems MS-BAIKAL2.
107). Magic Systems MS-156 MS-22531).
108). Scher-khan Logikar 1, Logikar 2, Logikar 3, Logikar 4, C, D MAGIC CODE™ PRO.

У наведеному переліку типів автосигналізацій визначено, що наданий кодграббер на базі пульта автомобільної сигналізації «Sheriff ZX-1095 PRO» має можливість відтворення роботи сигналізації типу «Sheriff», якою було обладнано наданий автомобіль. Наведений список не є повним у зв'язку з постійними оновленнями програмного забезпечення кодграбберів та бази даних роботи алгоритмів шифрування.

Кодграббери, побудовані на базі пульта автомобільної сигналізації «Sheriff ZX-1095 PRO», мають такі технічні характеристики:

- дисплей РКЕ;
- 9 комірок пам'яті;
- підтримка режиму "Автозапуск";
- відкриття багажника;
- PIN-код на включення;
- блокування зворотного зв'язку на пульті оригінальної автосигналізації.

Перелік посилань

1. Інтернет-ресурс. Режим доступу: http://130.com.ua/product/car-alarm-sheriff-zx-1095-two-way-and-remote-engine-start/
2. Інтернет-ресурс. Режим доступу: http://www.aliexpress.com/price/pl2303hx-arduino_price.html
3. Інтернет-ресурс. Режим доступу: http://www.prolific.com.tw/US/ShowProduct.aspx?pcid=41&showlevel=0017-0037-0041

ИССЛЕДОВАНИЕ АЛГОРИТМИЧЕСКОГО КОДГРАББЕРА

Г. В. Куцо

Для проникновения в автомобиль - «взлома» автосигнализации похитителями используются кодграбберы («code grabber», «перехватчик кода»). Различают три типа подобных устройств: кодграббер для статических кодов, кодграбберы по принципу кодоподмены (для одно- и двухкнопочных брелоков) и алгоритмические (иногда их называют «мануфактурными»).

Для более ранних систем автосигнализации, которые используют статический код, достаточно устройства, которое перехватывает этот код и запоминает его.

Для кодграбберов, основанных на принципе кодоподмены, характерен алгоритм работы, который требует повторного нажатия владельцем кнопок брелока, используя частично одновременно радиоглушение и перехват сигнала брелока.

Алгоритмический кодграббер — устройство, которое распознает по цифровому сигналу брелока тип (то есть производителя, «бренд») сигнализации и, используя так называемый «Мануфактурный код», становится клоном (полным дубликатом) брелока владельца. Этот принцип применяется к автосигнализации, использующей алгоритм KeeLoq и др. для кодировки сигнала от брелока к центральному блоку сигнализации и по радиообмену «брелок — центральный блок» (диалоговые системы). Считается, что мануфактурные коды («коды изготовителя») для большинства типов сигнализаций получены методами промышленного шпионажа на заводах (преимущественно в Китае), которые осуществляют программирование микроконтроллеров систем автосигнализации, или в результате обратной инженерной разработки чипов микроконтроллеров. Существуют «черные списки» автосигнализаций, которые раскрываются алгоритмическим кодграббером. Такой кодграббер, в зависимости от функций и количества «прошитых» автосигнализаций, продается для тестирования сигнализаций в автосервисах и страховых компаниях. Наиболее подвержены взлому кодграббером охранные системы без диалогового кода с индивидуальными ключами шифрования.

Эта статья освещает последовательность проведения исследований алгоритмического кодграббера на базе пульта автомобильной сигнализации “Sheriff ZX-1095 PRO” и дает возможность оперативного определения признаков перепрограммирования пульта автомобильной сигнализации “Sheriff ZX-1095 PRO”. В данной статье приведены совокупные признаки сканеров, грабберов, кодграбберов, алгоритмических кодграбберов.

Представленный в статье алгоритмический кодграббер не отличается от пульта автомобильной сигнализации по внешним признакам. Автором приведены внешние признаки, по которым можно оперативно отличить пульт автосигнализации от представленного кодграббера, основанного на базе пульта автомобильной сигнализации “Sheriff ZX-1095 PRO”. Это даст возможность оперативно проводить внешний осмотр та отличать пульт автосигнализации от представленного алгоритмического кодграббера.

Для автовладельцев следует отметить, что на сегодняшний день не существует абсолютной защиты от кодграбберов. Только использование комплексных мероприятий поможет автовладельцу защитить его автомобиль от незаконных посягательств, но это станет темой следующих публикаций.

RESEARCH ALGORITHMIC CODE GRABBER

G. Kutso

Robbers use “code grabbers” to penetrate the car and “hack” the car alarm system. There are three types of such devices, namely code grabber for static codes, code grabber on the principles of code substitution (for one- and two-button keychains) and algorithmic (sometimes they are called “manufacturing”).

For earlier car alarm systems using the static code, it is enough to use the device that captures this code and remembers it.

For code grabbers based on the principles of code substitution, the characteristic algorithm of operation, which requires repeated pushing of keychain buttons by the owner, is based on partially simultaneous radio jamming and capture of the keychain signal.

Algorithmic code grabber is a device that recognizes the type (namely, the manufacturer, “brand”) of an alarm system by the digital signal of the keychain, and becomes a clone (total duplicate) of the owner’s keychain using the so called “Manufacturer’s code”. This principle is applied to the car alarm system, which uses the algorithm KeeLoq etc. for coding a signal from

the keychain to the central alarm system block and radio exchange “keychain-central block” (dialogue systems). It is believed that manufacturing codes (“manufacturer’s codes”) for most types of alarm systems are received by methods of industrial spying in factories (mainly in China), that carry out programming of microcontrollers of car alarm systems, or due to reverse engineering design of microcontrollers chips. There are “black lists” of car alarm systems, which can be hacked by algorithmic code grabber. Such code grabber, depending on the functions and quantity of “threaded” car alarm systems, is sent for testing an alarm system in car service centers and insurance companies. Security systems most attackable by the code grabber are without a dialogue code with individual coding keys.

This article highlights the consistency of research of algorithmic code grabber on the basis of remote car alarm “Sheriff ZX-1095 PRO” and gives an opportunity of operative determination of signs of reprogramming of remote car alarm “Sheriff ZX-1095 PRO”. This article presents collective signs of scanners, grabbers, code grabbers and algorithmic code grabbers.

Algorithmic code grabber described in the articles does not differ from the remote car alarm by its appearance. The Author presents external signs, according to which it is possible to effectively distinguish the remote car alarm from the above-mentioned code grabber, which is produced on the bases of the remote car alarm system “Sheriff ZX-1095 PRO”. This will give an opportunity to effectively conduct an external review and distinguish the remote car alarm system from the above-mentioned algorithmic code grabber.

It should be noted for car owners, that nowadays absolute protection from code grabbers does not exist. Only complex measures will help a car owner to protect his/her car from unlawful attacks, but this is the topic of the following publications.

УДК 343.982.323

А. С. Джавадян
кандидат медицинских наук,
директор

П. С. Восканян
кандидат химических наук,
заместитель директора

Национальное бюро экспертиз Республики Армения

ПРИМЕНЕНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННЫХ СУДЕБНО-ЭКСПЕРТНЫХ ИССЛЕДОВАНИЯХ

В статье отмечено, что для проведения экспертных исследований и повышения их доказательной значимости, необходимо наличие соответствующих методик, основанных на использовании современных достижений науки и техники, позволяющих получать объективные документированные результаты измерений.

В условиях всеобщей информатизации и глобальной компьютеризации всех сфер жизнедеятельности человека наиболее значимые и актуальные