УДК 004.62+004.77

А.О. Аносов, А.В. Платоненко

МОДЕЛЬ ПЕРЕХОПЛЕННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ

Розглянуто вразливості бездротових мереж, шляхи перехоплення інформації та впливу на бездротову мережу, а також методи та засоби захисту, що можуть використовуватись для запобігання від несанкціонованого доступу, який несе за собою небезпеку для інформації, що зберігається та передається з використанням сучасних мобільних пристроїв.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв.

Вступ

Неуважні, або недосвідчені користувачі мобільних пристроїв випадково встановлюють зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисники можуть отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, можливості зловмисників збільшуються в рази.

Основна частина

Небезпеку для інформації несуть відкриті Wi-Fi мережі, адже кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись його у працівника.

Ненадійні паролі зазвичай стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, він отримує доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки.

Загальну модель перехоплення та захисту інформації в бездротових мережах зображено на рис. 1., де структурно відображені можливі шляхи перехоплення та захисту інформації.

1. Стандартна взаємодія пристрою з глобальною мережею через роутер (нормальний стан). Модель описує нормальний стан роботи мережі, інформація з мобільного пристрою передається через бездротову мережу, без втручання зловмисника.

2. Вплив зловмисника на бездротову мережу з метою перехоплення інформації з пристрою. В даному випадку бездротова мережа піддається впливу зловмисника. Розглядається вплив на об’єкт з використанням локальної бездротової мережі. Зловмисник з використанням спеціального програмного та апаратного забезпечення намагається проникнути в мережу. Метою таких дій є бажання отримати доступ до мережі, що може дати йому змогу перехоплювати інформацію з пристроїв підключених до мережі. Також зловмисник може змінювати параметри об’єкта таким чином, що клієнт мережі може нічого не помітити, але буде передавати зловмиснику свої дані, чи відвідувати саме ті ресурси, в яких зацікавлений зловмисник.

3. Засоби захисту адміністратора для бездротової мережі. При взаємодії клієнта мережі через об’єкт можливі декілька сценаріїв роботи, а саме:

- без використання шифрування, відкрита мережа, до якої може підключитись кожен;
- з використання шифрування (WEP, WPA/WPA2 – Personal, WPA/WPA2 – Enterprise).

Окрім даних інструментів адміністратор може використовувати ще додаткові програмні (антивірусне програмне забезпечення, сканер мережі, брандмауер) та програмно-апаратні засоби (NGFW, Radius-server, хмарні сервіси).

Дані інструменти захисту можуть працювати окремо, або взаємодіяти між собою, окрім цього більшість з них має можливість захистити від впливу з глобальної мережі (п.5, 11).

4. Вплив зловмисника на інформацію через глобальну мережу та вразливості зв'язку між нею та роутером.

Якщо адміністратор мережі лишив налаштування об'єкту «за умовчуванням», або не встановив захищені налаштування, то вплив на локальну бездротову мережу можливий віддалено, з використанням глобальної мережі та вразливості в налаштуваннях. Таким чином зловмисник може впливати на конфігурацію та налаштування бездротової мережі перебуваючи навіть в іншій країні.

5. Засоби захисту адміністратора для каналу зв'язку між глобальною мережею та роутером.

Завдяки використанню стійкого пароля та зміни логіна для доступу до налаштувань, обмеження кількості спроб авторизації та забороні доступу до налаштувань локальної мережі з використанням глобальної, адміністратор може мінімізувати можливості зловмисника. Для додаткового захисту необхідно використовувати програмно-апаратні засоби.

6. Прямий вплив зловмисника на адміністратора через бездротову мережу.

Завдяки використанню спеціальних програмних та програмно-апаратних засобів, зловмисник може видавати себе за адміністратора мережі та виконувати зловмисні дії від його лиця, окрім цього можливе блокування або створення перешкод для захисту.

7. Засоби протидії адміністратора від прямого впливу зловмисника на бездротову мережу.

Завдяки програмним та програмно-апаратним засобам адміністратор може не тільки захистити мережу від проникнення, а і обмежити доступ та захистити себе від нападу зловмисника.

8. Прямий вплив зловмисника на адміністратора через глобальну мережу.

Використовуючи зловмисне програмне забезпечення та вразливості в налаштуваннях зловмисник може задіяти глобальну мережу та виконувати дії аналогічні п.6.

9. Засоби протидії адміністратора від прямого впливу зловмисника на глобальну мережу.

Аналогічно до п.7, адміністратор повинен захищати мережу від впливу через глобальну мережу.

10. Вплив зловмисника на бездротову мережу через глобальну з використанням хмарних технологій.

З використанням сучасних хмарних технологій зловмисник може виконувати необхідні йому обчислення для злому на віддалених, але високопродуктивних програмно-апаратних засобах.

11. Захист бездротової мережі адміністратором через глобальну з використанням хмарних технологій.

Завдяки використанню сучасних хмарних технологій адміністратор також має програмно-апаратні засоби, які дозволяють йому аналізувати та відслідковувати спроби несанкціонованого доступу завдяки спеціальним хмарним сервісам.

12. Захист бездротової мережі адміністратором з використанням RADIUS-SERVER.

Для конфігурації локальної мережі підприємства використовується дана модель захисту, яка робить практично не можливим перехоплення інформації в захищеній мережі.

13. Захист бездротової мережі адміністратором з використанням NGFW.

З використанням даного програмно-апаратного засобу можна захистити мережу як локально, так і від впливу з глобальної мережі, а також з використанням хмарних сервісів, що дає змогу поєднати в собі інструменти описані в п. 3, 5, 7, 9, 11, що робить його універсальним засобом моніторингу та захисту мережі, як локальної, так і глобальної.

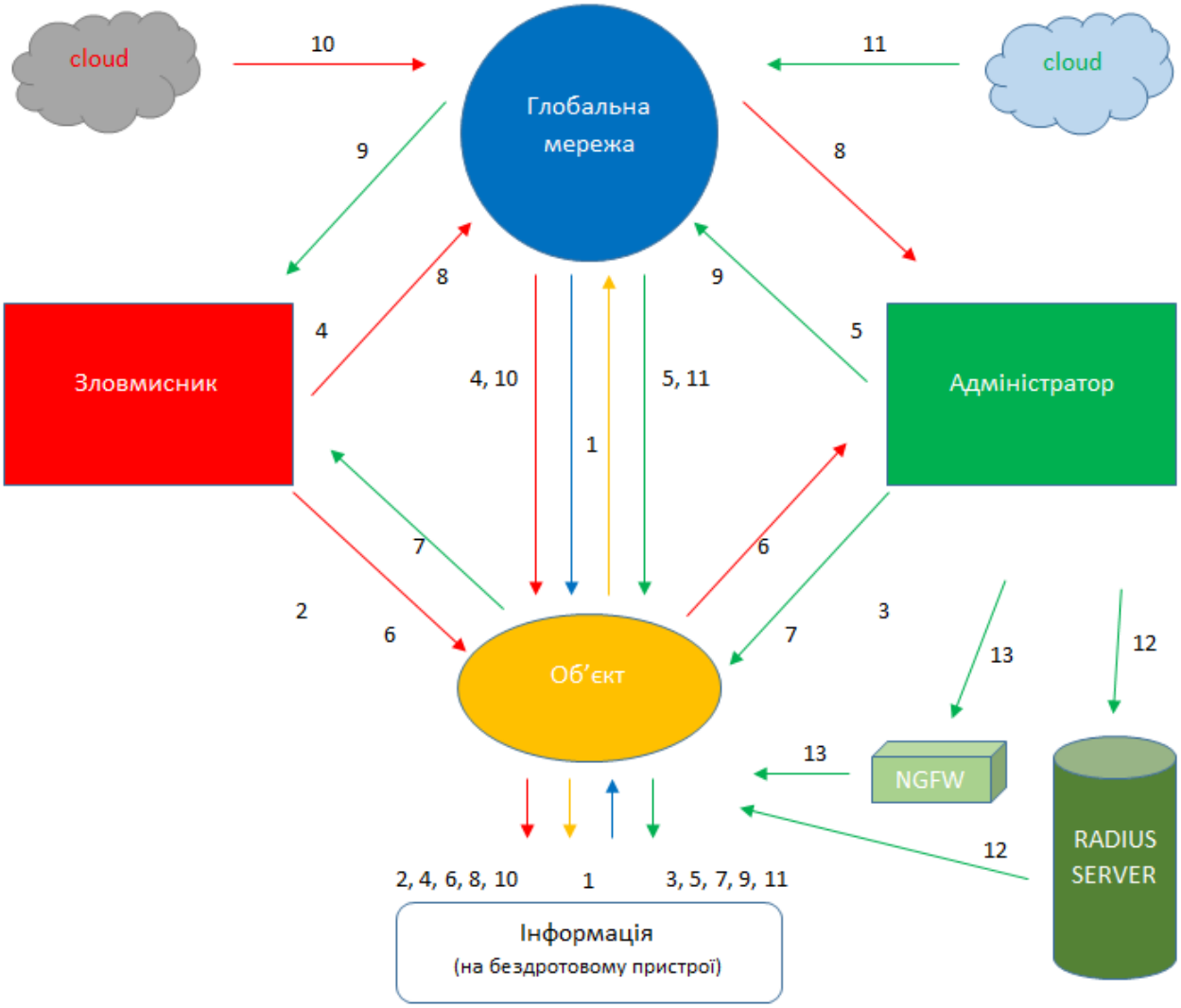

Рис.1. Загальна модель перехоплення та захисту інформації в бездротових мережах

На підставі розглянутих чинників постає задача у вигляді пошуку «надійного» пароля для захисту інформації в бездротових мережах, яке в загальному вигляді може бути представлено виразом:

$$\{\{X\}, O(P)\} \rightarrow z \qquad (1)$$

де { *X* } - множина паролів;
O – правило, яке встановлює перевагу на множині паролів,
Pv – ймовірність злому,
z – обраний пароль.

Критерієм вибору паролю є мінімальна ймовірність його підбору.

$$O(P) \rightarrow 0 \qquad (2)$$

Чим більша стійкість паролю – тим менша ймовірність підбору (Z) і навпаки, більша ймовірність підбору – означає меншу стійкість паролю.

Статистичною (емпіричною) функцією розподілу вибірки множини паролів є закон зміни частоти події підбору пароля, при $X<x$:

$$^*(x) = \frac{n(x)}{n}, \qquad (3)$$

де $n(x)$ – число значень варіантів паролю, для яких $x \leq X$,

X –випадкова величина множини паролів, розподіл якої невідомий;
n – об'єм вибірки множини паролів.

Аналогом теоретичної диференціальної функції (густини) розподілу є щільність відносної частоти:

$$f_i = \frac{W_i}{h} \quad (4)$$

де W_i – відносна частота , h – інтервал підбору.

На відміну від емпіричної функції розподілу вибірки множини паролів функція розподілу *F(x)* генеральної сукупності їх множини є теоретичною функцією розподілу.

Різниця між ними полягає в тому, що теоретична функція F(x) визначає ймовірність підбору X<x, а емпірична функція F*(x) визначає відносну частоту цього ж підбору.

Емпірична (статистична) функція розподілу вибірки множини паролів є оцінкою теоретичної функції розподілу генеральної сукупності їх множини.

Математичне сподівання характеризує середнє значення, біля якого групуються можливі значення випадкової величини підбору, а дисперсія характеризує степінь розсіювання цих значень відносно середнього.

Середнє арифметичне спостережуваних значень випадкової величини множини паролів:

$$M^*[X] = \frac{\sum_{i=1}^{k} x_i\, n_i}{n} = x_e \quad (5)$$

де x_i – значення випадкової величини паролю,

$n = \sum_{i=1}^{k} n_i$ - число випробувань можливого підбору (об'єм вибірки).

Статистичні початкові та центральні моменти вибірки довільних порядків *m*:

$$M[(X - x_r)^m] = \frac{\sum_{i=1}^{k} (x_i - x_r)^m N_i}{N} \quad (6)$$

При збільшенні числа спостережень вибірки множини паролів всі статистичні характеристики будуть збігатись за ймовірністю до відповідних числових характеристик генеральної сукупності їх множини.

При M →Max, Pv → 0

Для даних паролів можливі деякі відмінні за кількістю множини.

Сполучення множини паролів (комбінація). З n елементів вибирають k, порядок не має значення.

$$C_n^k = \frac{n!}{(n-k)! \cdot k!} \quad (7)$$

де n- кількість можливих символів;
k- довжина обраного паролю.

Розміщення множини паролів. З n елементів вибирають k в певному порядку.

$$A_n^k = \frac{n!}{(n-k)!} \quad (8)$$

де n- кількість можливих символів;
k- довжина обраного паролю.

Розміщення з повтореннями множини паролів. Число всіх розміщень з n по k з повтореннями.

$$A'^k_n = n^k \quad (9)$$

де n- кількість можливих символів;
k- довжина обраного паролю.
В даному випадку:

n=88 - ASCII: 26 прописних літер, 26 заголовних літер, 10 цифр, 26 спеціальних символів;

k=63 - кількість символів у паролі для WPA/WPA2.

Таблиця 1

Кількість паролів, що можуть використовуватись для захисту бездротових мереж

Вид захисту	**Кількість символів в паролі**	**Можлива кількість паролів**	
WPA/WPA2 (TKIP 128 біт)	63 символи ASCII	Сполучення	$6.03 \cdot 10^{21}$
		Розміщення	$1.19 \cdot 10^{109}$
		Розміщення з повтореннями	$3.18 \cdot 10^{122}$

Висновки

Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації вирішується навчанням правилам інформаційної безпеки. Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів.

Методи підвищення захищенності бездротових мереж шляхом використання надійного паролю, його генерування та перевірки на унікальність й складність будуть розглянуті в наступних роботах.

Список використаної літератури

1. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах/ А. В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р.

2. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко, Київ, ДУТ, Сучасний захист інформації. Науковий журнал. – 2015. – № 4, с. 86 – 90.

3. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

4. Некоторые интересные факты о подборе паролей [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153530.

5. Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers [Електронний ресурс] – Режим доступу: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious-firmware-update-to-32-million-home-routers.

Надійшла 18.01.2017 р. Рецензент: д.т.н., проф. Шевченко В.Л.