УДК 004.7 + 004.056 Вестник УрФО № 4(18) / 2015, стр. 16–20

Токарчук Е. Д., Зюляркина Н. Д.

АНАЛИЗ ЗАЩИЩЕННОСТИ МЕХАНИЗМОВ ПОДКЛЮЧЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ К СЕТЯМ WI-FI

Работа посвящена вопросам безопасности поиска и подключения к открытым Wi-Fi сетям на мобильных устройствах, а в частности рассматривается вопрос автоматического подключения к Wi-Fi сетям, имеющим одинаковый SSID сети. Так как данная особенность подключения к открытым Wi-Fi сетям позволяет злоумышленникам производить атаки на клиентские устройства, например атаки типа MITM, в работе предлагается прототип клиентского приложения, которое бы осуществляло дополнительную проверку Wi-Fi сети, направленную на защиту клиентского устройства, информирование пользователя об автоматическом подключении к открытой Wi-Fi сети, а также принудительное отключение пользователя от сети, представляющей потенциальную угрозу для пользователя.

Ключевые слова: *информационная безопасность, сети, Wi-Fi, android.*

Tokarchuk E. D., Zyulyarkina N. D.

ANALYSING SMARTPHONE WI-FI CONNECTING MECHANISM SECURITY

The work is dedicated to the issues of WiFi search and connection safety mechanisms on mobile devices, in particular it is concerned with the question of automated connection to public Wi-Fi networks, which have an identical network SSID. Since this public Wi-Fi connection feature allows attackers to make attacks on clients' devices, for example the MITM attack, this paper proposes a client application prototype, which would make additional public Wi-Fi network verification, concerning the protection of a client's device, informing the user of the automatic connection to a public Wi-Fi network and a forced disconnection from a potentially dangerous network.

Keywords: *information security, networks, public Wi-Fi, android.*

	Data Consumption [MB/month]			User Growth	Data Growth
Device Type	**2010**	**2011**	**2016**	**[CAGR 2011-16]**	**[CAGR 2011-16]**
Non-smartphone	1.9	4.3	108	-	-
E-reader	0.5	0.73	2.8	-	-
Smartphone	55	150	2,576	24%	119%
Portable gaming console	244	317	1,056	56%	76%
Tablet	405	517	4,223	50%	129%
Laptop and netbook	1,460	2,131	6,942	17%	48%
M2M module	35	71	266	42%	86%

Рис. 1. Рост количества трафика на различных устройствах

Основная идея

В настоящее время Wi-Fi сети составляют превалирующую часть всех сетей. На развитие Wi-Fi инфраструктуры повлиял рост количества мобильных устройств, для которых этот способ предоставления услуг доступа к сети является основным. По прогнозам экспертов Cisco [1], к 2016 году трафик беспроводных устройств значительно превысит трафик проводных (рис. 1).

Однако с ростом количества открытых сетей и мобильных устройств, подключающихся к ним, растет и количество атак на мобильные устройства через эти сети. Основными атаками в открытых сетях доступа являются атаки типа Man-In-The-Middle. В данной работе рассмотрены механизмы поиска и подключения в сетях Wi-Fi, а также предложен вариант приложения для защиты мобильного устройства в таких сетях.

Активное сканирование. Proberequest

Для обнаружения доступных сетей клиентские устройства могут использовать два режима:

• пассивное сканирование — прослушивание beacon-фреймов от точки доступа;

• активное сканирование — отправка фреймов типа proberequest [2].

В настоящее время все мобильные устройства совмещают активное и пассивное сканирование для обнаружения Wi-Fi сетей. В данной работе рассматривается только активное сканирование.

При активном сканировании данный фрейм отправляется устройством на mac-адрес ff:ff:ff:ff:ff:ff. При отправке фрейм может как содержать SSID сети (directproberequest), так и отправляться с SSID=0 (nullproberequest). Схема работы механизма proberequest представлена на рис. 2

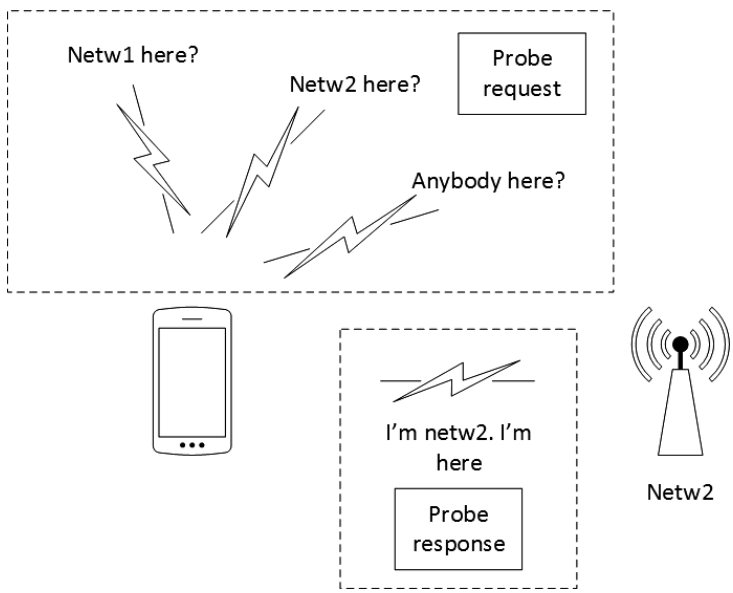

Рис. 2. Схема активного сканирования сети

map it	netid	ssid	firsttime	lasttime	wep	trilat	trilong	lastupdt	channel	qos
Get Map	0C:D9:96:83:D7:D1	SUSU_EDU	1970-01-01 05:00:00	2014-03-17 10:13:15	2	55.15941620	61.36962509	20140317081331	1	3
Get Map	0C:D9:96:83:D7:D2	SUSU_EDU	2013-02-03 14:39:11	2013-08-30 00:05:14	?	55.15927887	61.36960602	20131013040705	11	2

Рис. 3. Часть результатов поиска сети SUSU_EDUв Wigleonlinedatabase

Если мобильному устройству удалось найти сеть, к которой он уже производил подключение, то подключение к такой сети происходит автоматически. Android устройства не предоставляют возможности указать в настройках отмену автоматического подключения к сети, однако можно в ручном режиме «забыть сеть».

Атаки типа MITM

Фреймы proberequest могут перехватываться злоумышленником, который осуществляет сниффинг трафика, таким образом, злоумышленник получает доступ к SSIDWi-Fi сетей, к которым подключалось устройство. В данной работе было осуществлено исследование этого механизма.

Для осуществления перехвата фреймов использовались:

1. ПК (ArchLinux kernel 3.18.6);
2. RaspberryPi (Pidora);
3. aircrack-ng;
4. Скрипт hoover.pl, являющийся оберткой над tshark.

ПК и RaspberryPi осуществляли мониторинг сети в разных точках города в течение рабочего дня. За это время было обнаружено 73 устройства, рассылающих proberequest (с уникальным mac-адресом) и 143 сети (с уникальным SSID).

Используя WirelessNetworkMapping сервис (например, wigle.net) на основе SSID, можно получить не только местонахождение данной AP, но и дополнительную информацию, такую как тип шифрования, BSSID, номер канала и т. д. (рис. 3).

Всю полученную информацию можно использовать для проведения атак типа MITM, т. к. обычно мобильные устройства автоматически подключаются к знакомым сетям и, если данная сеть является открытой, для осуществления атаки Man-in-the-Middle достаточно создать точку доступа с таким же SSID, который отправляется жертвой в proberequest. Первыми о возможности такой атаки написали D. A. DaiZovi и S. A. Macaulay в своей статье “Attacking automatic wireless network selection” в 2005 году [3]. Ими был разработан набор утилит KARMA для осуществления подобных атак.

Однако стоит отметить, что в версиях android 4.1 и выше при отправке фреймов proberequest SSID остается нулевым. Таким образом, невозможно определить, какую

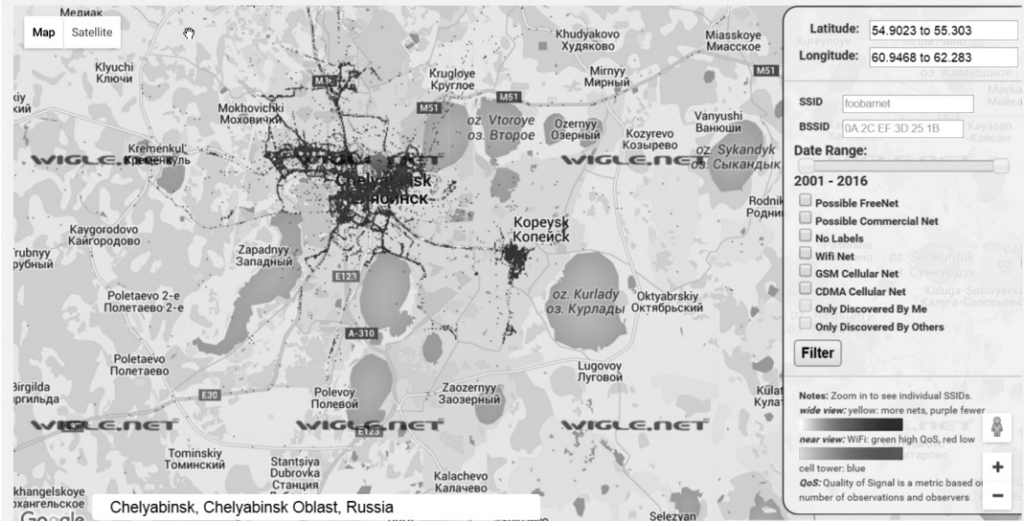

Рис. 4. Карта Wi-Fi сети города Челябинска

сеть пытается найти устройство, и уж нельзя осуществить направленную атаку Man-in-the-Middle и определить расположение Wi-Fiточки доступа. Об этом изменени и говорятв своем докладе на конференции Defcon “Manna from heaven: Improvements in Rogue AP attacks” [4] Dominic White и Ian de Villiers. Они предложили улучшенную версию KARMA для осуществления атак типа MITM.

С другой стороны, можно сделать поиск открытых сетей в пределах некоторых координат, и таким образом получить список открытых Wi-Fi сетей и попытаться совершить атаку Man-in-the-Middle, исходя из предположения, что пользователь возможно уже подключался к сети. Существуют такие открытые Wi-Fi сети провайдеров, которые имеют один и тот же SSID для всех точек доступа, что увеличивает вероятность подключения пользователя к ней. На рис. 4 показана карта Wi-Fi сети города Челябинска (как открытые, так и частные сети).

Идея приложения

Открытые Wi-Fi сети предоставляют некоторую угрозу для безопасности мобильного устройства, однако сложно отказаться от преимуществ развитой Wi-Fi инфраструктуры, т. к. интернет стал неотъемлемой частью жизни и коммуникаций. Поэтому в данной работе предложен вариант создания приложения для OSAndroid, которое позволяет защитить и предупредить атаки типа MITM. Данное приложение должно иметь следующие основные функции:

- отслеживать Wi-Fi подключения;
- сохранять в сети SSID, BSSID точки доступа, дату последнего подключения и данные о местоположении точки доступа;
- если это сохраненная сеть, проверять не только SSID, но также BSSID сети и координаты (учитывая погрешность);
- если данная сеть предположительно навязана злоумышленником, отключать от нее принудительно и уведомлять пользователя.

Приложение должно действовать в фоновом режиме незаметно для пользователя. Такие меры могут помочь защититься от атак типа MITM в открытых Wi-Fi сетях, продолжая полностью использовать все их преимущества.

Для получения всей необходимой информации будут использоваться классы WifiInfo и LocationManager, предоставляемые APIAndroid. Информация будет сохраняться на устройстве в локальном хранилище приложения. Для того чтобы была возможность собирать необходимые данные, приложение должно иметь права на доступ к местоположению, доступ к состоянию сети и доступ к состоянию Wi-Fi подключения.

При подключении к какой-либо сети приложение будет получать уведомление с помощью класса BroadcastReceiver, что позволит инициировать проверку этой сети. Сеть, к которой подключается пользователь, будет искаться в списке сохранённых сетей и, если совпадения будут найдены, будут проверены дополнительные данные. На основании такой проверки будет сделан вывод о безопасности сети. При отсутствии такой сети в локальной базе она автоматически добавится в список, при этом если сеть открытая, пользователь будет предупрежден о возможной опасности.

Заключение

В магазине приложений Android существует множество программ – анализаторов сети, однако ни одно приложение не направлено на защиту от возможных атак, а только предоставляет ограниченные сведения о близко расположенных Wi-Fi сетях. Описанное в работе приложение позволит сократить риски от предполагаемых атак типа MITM в сетях открытого доступа и предупредить пользователя о возможной опасности. В настоящее время описанное в работе приложение находится на стадии разработки. В дальнейшем планируется закончить работу над приложением и выложить результат в AndroidPlayMarket.

Примечания

1. Settey V. Evolúciabezdrôtovýchtechnológií. CiscoExpo 2012, 76 p.

2. Geier, JimUnderstanding 802.11 Frame Types //Wi-Fi Planet.—http://www.wi-fiplanet.com/tutorials/print.php/1447501/

3. Dai Zovi, D. A., Macaulay, S.A. Attacking Automatic Wireless Network Selection//Information Assurance Workshop. 2005. —Pp. 365–372.

4. White, D., de Villiers, I. Manna from Heaven; Improving the state of wireless rogue AP attacks // Defconconference. № 22. 2014.

ТОКАРЧУК Евгения Дмитриевна, студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университ. 454080, г. Челябинск, проспект Ленина, 76. E-mail: evgeniya@tokarch.uk

ЗЮЛЯРКИНА Наталья Дмитриевна, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университ, д-р физ.-мат. наук. 454080, г. Челябинск, проспект Ленина, 76. E-mail: toddeath@yandex.ru

TOKARCHUK Evgeniya, student of the department «Security of information systems» South Ural State University, Bld. 76, Lenin prospekt, Chelyabinsk, 454080. E-mail: evgeniya@tokarch.uk

ZYULYARKINA Natalya, professor of department «Security of information systems» South Ural State University, Bld. 76, Lenin prospekt, Chelyabinsk, 454080. E-mail: toddeath@yandex.ru