8. Проект OSVDB [Электронный ресурс] URL: http://osvdb.org/ (дата обращения: 12.08.2013).
9. *Tumoyan E., Kavchuk D*. The method of optimizing the automatic vulnerability validation // Proceedings of the Fifth International Conference on Security of Information and Networks SIN 2012. – 25-27 October 2012. – P. 205-208.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Кавчук Дарья Александровна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: dar.ushka.k@gmail.com; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; аспирантка.

Тумоян Евгений Петрович – e-mail: e.tumoyan@gmail.com; кафедра безопасности информационных технологий; к.т.н.; доцент.

Евстафьев Георгий Александрович – ООО "Комплексные программные решения"; e-mail: gaevstafiev@yahoo.com; 347900, г. Таганрог, Мариупольское шоссе, 27/2, кв. 305; тел.: 88634605377; инженер-программист.

Kavchuk Daria Alexandrovna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: dar.ushka.k@gmail.com; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; postgraduate student.

Tumoyan Evgenie Petrovich – e-mail: e.tumoyan@gmail.com; the department of security in data processing technologies; cand. of eng. sc.; associate professor.

Evstafiev Georgyi Alexandrovich – OOO "Complex Program Solutions"; e-mail: gaevstafiev@yahoo.com; 27/2, Mariupolskoe shosse, apt. 305, Taganrog, 347900, Russia; phone: +78634605377; programming engineer.

УДК: 004.056

М.А. Кобилев, Е.С. Абрамов

РАЗРАБОТКА АЭРОМОБИЛЬНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ВЫСОКОЙ ФИЗИЧЕСКОЙ ЗАЩИЩЁННОСТЬЮ*

Описываются эксперименты по созданию прототипа лёгкого малозаметного летательного аппарата для проведения удаленного аудита безопасности информационных систем [пентеста]. Была предложена модификация квадрокоптера Parrot AR.Drone 2, предполагающая рациональное использование устройства в задачах анализа безопасности. Прототип работает под управлением Raspberry Pi, дополнительно используется специализированный беспроводной сетевой адаптер ALFA AWUS036NHR с направленной антенной и GPS-приёмник.

Рассмотрены возможные алгоритм функционирования атакующей системы. Предполагается использование прототипа в двух режимах - активного аудита и сервера-ретранслятора. В режиме аудита квадрокоптер непосредственно осуществляет атакующее воздействие на целевую сеть. В режиме ретранслятора квадрокоптер может становится передающим сервером для других устройств, расширяя радиус действия комплекса, либо передавая данные для анализа на мощный стационарный сервер.

* Работа выполнена при поддержке гранта РФФИ № 12-07-00014-а.

Результат исследования дал возможность создания как пилотируемого, так и беспилотного летательного аппарата, способного проникать на охраняемую территорию в целях аудита безопасности или атаки.

Квадрокоптер; AR.Drone; пентест; атака; несанкционированный доступ; беспроводные сети.

M.A. Kobilev, E.S. Abramov

DEVELOPMENT OF AIRMOBILE COMPLEX FOR SECURITY AUDIT OF INFORMATION SYSTEMS WITH HIGHLY PHYSICAL SECURITY

The paper describes experiments on a prototype of lightweight low-profile aircraft for remote security audit of information systems [so-called pentest]. The topic is a modification of the Parrot AR.Drone quadrocopter 2, implying a rational use of the device for analysis of security. The prototype runs on Raspberry Pi, additionally using a dedicated wireless network adapter ALFA AWUS036NHR with a directional antenna and a GPS-receiver.

The possible attacking algorithms were developed. Assumes the use of a prototype in two modes – active audit and the relay server . In audit mode, quadrocopter is involved in the attacking impact on the target network. In relay server mode quadrocopter can forward traffic to the server for other devices , extending the range of the complex or transmitting the data for analysis on the powerful stationary server.

The result of the study made it possible to create both manned and unmanned aircraft, able to penetrate the protected area for security audit or attack.

AR.Drone; UAV; Raspberry Pi; pentest; attack; unauthorized access; wireless networks; quadrocopter.

Введение. Основная задача пентестера – проникновение на вражескую территорию, но на пути к её решению всегда стоят непреступные крепости, обнесенные огромным забором с колючей проволокой по периметру, множеством камер видеонаблюдения и штатных охранников возле ворот с надписью «не входи – убьет». Увидев такой форт, пентестер приходит в недоумение – «а вдруг правда убьет?». Проникнуть незаметно становится невозможным – осада ведется крайне долго и безуспешно – все старания пропадают впустую.

На помощь приходят доступные и практичные летательные аппараты – мультикоптеры [1]. Они используются в киноиндустрии, в охранных [2] и почтовых службах [3], etc. Возможно и их применение в области информационной безопасности, а именно, пентеста [4, 5, 6].

1. Прототип. Устройство, выбранное для примера – Parrot AR.Drone 2 [7]. Основные характеристики представлены ниже, размеры и вес указаны на рис. 1. Отличительные особенности AR.Drone – наличие открытого API [8] и хорошее соотношение цена/качество.

Характеристики Parrot AR.Drone 2

Скорость: 5 м/с; 18 км/ч.

Время полета:

- 12 минут – LiPo 1000 mAh - время зарядки 90 минут.
- 25 минут – LiPo 2300 mAh - время зарядки 2–2,5 часа.

Управление: ограничен радиусом работы wifi (50–120 метров).

Аппарат приводится в движение четырьмя бесколлекторными 14.5 ваттными электромоторчиками 28 500 об/мин.

Безопасность:

- Автоматическая посадка при потере сигнала.
- Винты автоматически блокируются в случае контакта.
- Интерфейс управления позволяет немедленно остановить винты.
- Защитный кожух винтов для полёта в помещении.

Видео возможности:

- HD Видеокамера: 720p 30fps.
- Широкоугольная линза: 92 градуса.
- H264 формат кодирования видео.
- Видео передается и записывается на устройство управления или на usb-накопитель.
- Захват и сохранение изображений в JPEG (720p).

Электроника и датчики:

- Процессор 1GHz 32 bit ARM Cortex A8 с 800MHz video DSP TMS320DMC64x.
- Память 1Gbit DDR2 RAM на частоте 200MHz.
- Контроллеры моторов: 8 MIPS AVR CPU.
- Wi-Fi b/g/n.
- 3х осевой акселерометр.
- 3х осевой гироскоп с углом вращения 2000 градусов/сек.
- 3х осевой магнитометр с точностью до 6 градусов.
- Барометрический датчик с точностью +/- 10 Па (80см над уровнем моря).
- 60 fps вертикальная QVGA камера для измерения горизонтальной скорости.
- Ультразвуковые датчики для измерения высоты полета.
- Операционная система Linux 2.6.32.
- USB 2.0.

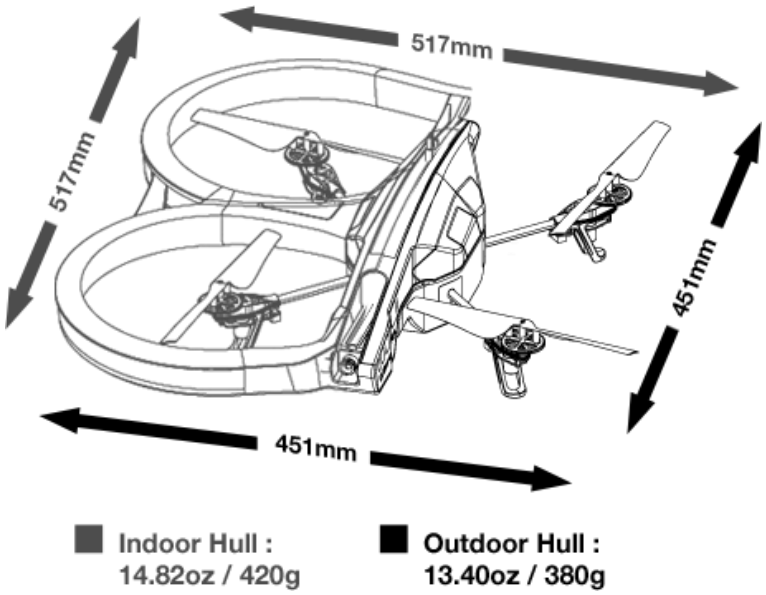

Рис. 1. AR.Drone:размеры и вес

2. Модификация AR.Drone. В стандартной комплектации AR.Drone больше походит на безобидное устройство. Для его вооружения я предлагаю провести ряд модификаций**.** Структурная схема модифицированного AR.Drone 2 проиллюстрирована на рис. 2.

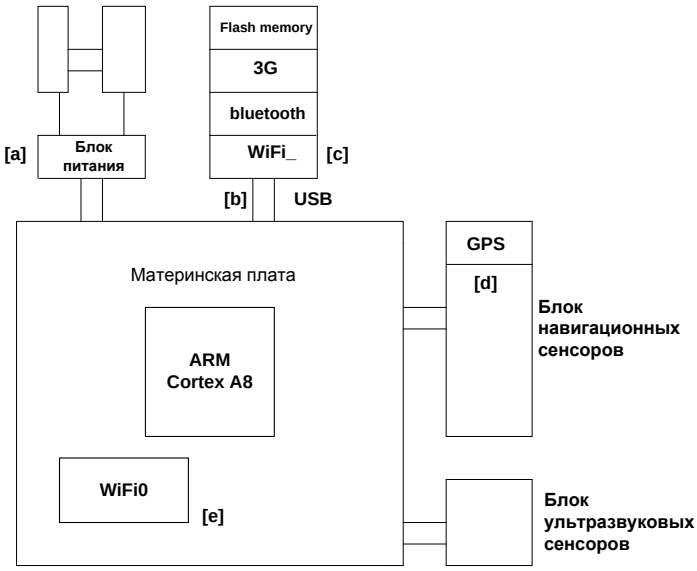

Рис. 2. Структурная схема модифицированного AR.Drone 2

Таблица 1

Характеристики дрона

AR. Drone 2	Raspberry Pi	ALFA AWUS036NHR	Flight Recorder
HD Camera. 720p 30fps 1GHz 32 bit ARM Cortex A8 processor with 800MHz video DSP TMS320DMC64x Linux 2.6.32 1Gbit DDR2 RAM at 200MHz USB 2.0 , Wi-Fi b/g/n Carbon fiber tubes : Total weight 380g with outdoor hull, 420g with indoor hull 4 brushless inrunner motors. 14.5W 28,500 RMP	SoC Broadcom BCM2835 (CPU, GPU, DSP, and SDRAM) CPU: 700 MHz ARM1176JZF-S core (ARM11 family) GPU: Broadcom VideoCore IV, OpenGL ES 2.0, 1080p30 h.264/MPEG-4 Memory RAM: 512 MB Video outputs: Composite RCA, HDMI Audio outputs: 3.5 mm jack, HDMI Onboard storage: SD, MMC, SDIO card slot 10/100 Ethernet RJ45 onboard network Wi-Fi with USB dongle SD/ MMC/ SDIO 2 USB port Power: 1mA at 5V Formfactor:85,6x54,0x17 mm	Standards Wireless: IEEE 802.11b/g/n Data Rate: 802.11b: UP to 11Mbps 802.11g: UP to 54Mbps 802.11n: UP to 150Mbps OS Supported: Win/Linux/Mac Interface: USB 2.0 Chipset: RTL8188RU Antenna: 5dBi 2.4GHz Antenna Antenna Type: 1 x 2.4Ghz RP-SMA Frequency Range: 2.412 ~ 2.483 GHz Channels: 1~14 Sensitivity: 11b: -96dBm 11g: -92dBm 11n: -91dBm Data Modulation Type: BPSK/QPSK/CCK/OFDM	Dimensions: 77.7 x 38.3 x 12.5mm Weight: 31g Accuracy: /- 2 meters Frequency: 5Hz Voltage: 3.3V TBC Time To First Fix: 25s maximum 4Gb Flash memory (allows 2 hours of video to be recorded) USB Port: Comprises one type A

8 MIPS AVR CPU per motor controller 3 elements 1000 mA/H LiPo rechargeable battery (Autonomy: 12 minutes) Emergency stop controlled by software Fully reprogrammable motor controller Water resistant motor's electronic controller	Total weight 45g	Power Voltage: 5V+5% Security: WEP/WPA/WPA2 Total weight 25g	female USB port to connect a USB key drive Total weight 15g

Рассмотрим подробнее предлагаемые модификации:

[a] – Стандартную батарею 1000mAh заменить на 2300 mAh –увеличит время полета с 12 до 25 минут. Поставить небольшой резервный источник питания, который обеспечит возможность срочной передачи данных на сервер (при разряде основной батареи) и удаление данных с Дрона в случае его обнаружения.

[b] – USB шина позволяет подключать дополнительные устройства:

- Флеш память (минимум 100 Мб свободного места и только в FAT32) нужна для сохранения видео.
- 3G – для передачи данных на сервер и получения команд.

[c] – WiFi_ Новый (Взамен WiFi0) интерфейс управления. Поддерживает алгоритмы защиты WEP/WPA – уменьшает вероятность «угона». PCB антенна 5–6 dBi для увеличения дальности приема.

[d] – GPS для автономной работы – автопилот и сохранения координат атакуемых сетей.

[e] – Интерфейс управления теперь служит для анализа. Антенны 2–3 dBi для этих целей вполне достаточно. При необходимости её можно заменить.

При модернизации дрона необходимо учитывать вес составных частей – перегрузка приведет к уменьшению времени полета, а уменьшение суммарного веса за счет замены деталей конструкции может в будущем привести к деформации корпуса при внешних воздействиях.

В случае потери связи с каналом управления wifi, квадрокоптер приземляется – при его обнаружении вражеская сторона получит все данные, хранящиеся в памяти устройства. Конечно же, ничего важного там храниться не будет, но для надежности канал управления необходимо дублировать по 3G, а дополнительный аккумулятор, в случае разрядки или отключения основного, позволит провести экстренное удаление данных.

3. Алгоритм функционирования квадрокоптера. Один из недостатков управления квадрокоптера AR.Drona – это необходимость присутствие человека. Эту проблему решает автопилот, например PX4FMU [9]. С таким устройством дрон сам может добираться до места атаки, но ему все еще не хватает знаний о поведении на вражеской территории.

Алгоритм, описывающий действия шпиона:

1. Летим до места атаки
2. Прилетели?
   - Да – goto 3
   - Нет
     - Заряда хватит?
       - Да – goto 1
       - Нет
         - Садимся – переходим в режим роутера
3. Ждем сигнала от сервера
   - Нужно атаковать?
     - Да – атакуем
   - Проводим анализ
   - goto 3
4. Летим домой

Листинг 1 – Алгоритм функционирования дрона

В режиме разведки (рис. 3) первый дрон (attacker_1) получает сигнал от сервера управления (attacker_serv) и отправляется в область предполагаемого присутствия жертвы (target_area). Оказавшись на контрольной точке, наш шпион начинает разведку местности – проводит анализ и выявляет области для возможного проведения атаки. Обнаружив беспроводные сети (target_1, target_2), сохраняет всю доступную информацию – месторасположения, области наилучшего уровня сигнала, защита, etc.

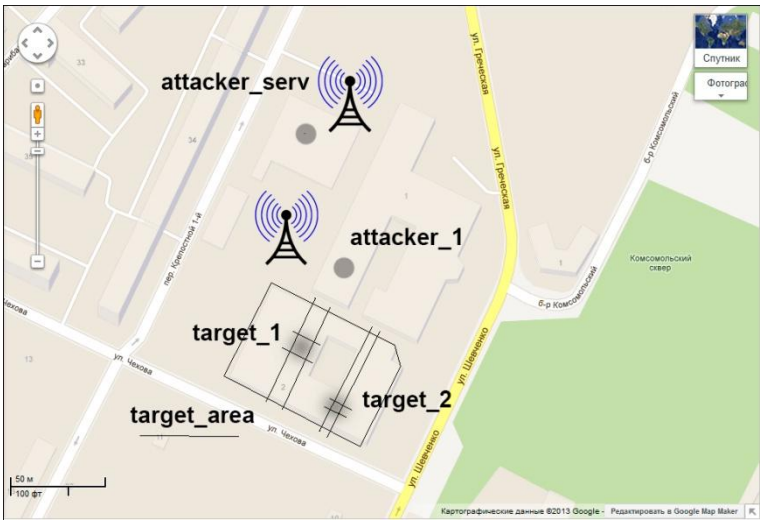

Рис. 3. Режим разведки

В случае если дрон начинает терять сигнал от сервера, он переходит в режим роутера (рис. 4), что позволяет транслировать управляющие сигналы далеко за пределы доступности сети сервера, использую промежуточные дроны в качестве ретранслятора. Такой сценарий используется, например, при следующих обстоятельствах: Первый дрон теряет сигнал от сервера и ему необходимо приземлиться в точке максимально приближенной к области атаки, но при этом с оптимальным уровнем связи с центром управления для трансляции второму дрону (attacker_2), который берет на себя обязанности по анализу и атаке.

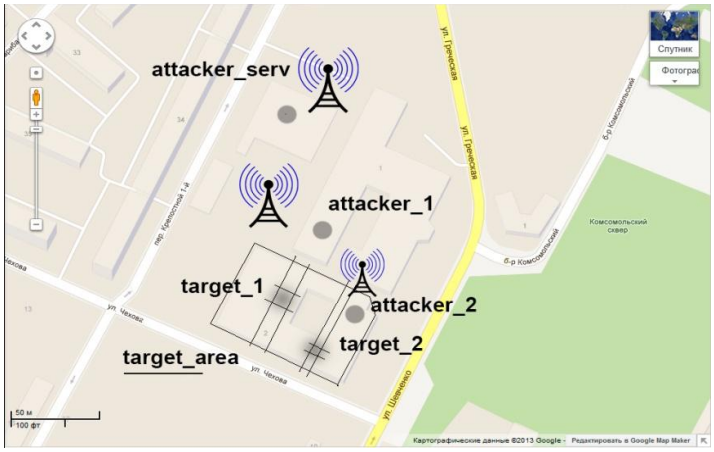

Рис. 4. Дрон в режим роутера

4. Анализ перехваченных данных и проведение атаки. Анализ системы состоит из нескольких этапов в зависимости от поставленной задачи:

1. Сбор информации о сетях:
   - ♦ Координаты сетей/уровень сигнала.
   - ♦ Оборудование/Защита.
   - ♦ Количество пользователей/etc.
2. Видео/фото/аудио съемка.

Вектора атаки выглядят следующим образом:

1. НСД
   - Сеть открыта?
     - Да
       - анализируем систему
       - проводим необходимые атаки
       - отправляем отчет серверу
     - Нет
       - WEP - AIRCRACK-NG [10]
       - WPA1/2 – gpuhash [11]
       - Goto 1
2. Заглушить сигнал 3G/WiFi/Bloototh.

Листинг 2 – Вектора атаки

Заглушив сигнал рабочей сети – можно прервать работу целого офиса. Одиночно или в совокупности с другими атаками (например, DoS) заглушка сигнала внутренней сети может привести к большим материальным потерям.

Заключение. В будущем размеры «летающих шпионов» будет уменьшаться: например, AR.Drone 2 кажется гигантом на фоне Crazyflie Nano [12], который может поместиться на ладони, однако его аккумулятора и тяги моторов пока недостаточно, чтобы поместить на своем борту весь арсенал пентестера. Пока с этой задачей могут справиться только устройства из класса «больших» мультикоптеров, но нанотехнологии стремительно развиваются и я не могу с уверенностью сказать, что будет завтра. А сегодня обычный, легко доступный квадрокоптер, при определенных модификациях и в умелых руках, может стать вполне серьезным инструментом пентестера, позволяющим скомпрометировать самые защищенные и неприступные инфокрепости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Quadrotor* [Электронный ресурс] // интернет-энциклопедия. Режим доступа: http://en.wikipedia.org/wiki/Quadrotor (Дата обращения: 13.05.2013).
2. *СТОРОЖЕВОЙ ДРОН: НА ПОСТУ* [Электронный ресурс] // Интернет-журнал «Популярная механика». Режим доступа: http://www.popmech.ru/article/12312-storozhevoy-dron/ (Дата обращения: 13.05.2013).
3. Во Франции появятся летающие почтальоны [Электронный ресурс] // Портал. Режим Доступа: http://24gadget.ru/1161053688-vo-francii-poyavyatsya-letayuschie-pochtalony-3-foto.html (Дата обращения: 13.05.2013).
4. Theodore Reed, Joseph Geis, Sven Dietrich. SkyNET: a 3G-enabled mobile attack drone and stealth botmaster. Stevens Institute of Technology, USA, 2011.
5. Hackers Turn The Parrot AR.Drone Into Aerial WiFi Hacking Rig [Электронный ресурс] // Новостной портал. Режим Доступа:http://toucharcade.com/2011/09/12/hackers-turn-the-parrot-ar-drone-into-aerial-wifi-hacking-rig/ (Дата обращения: 13.05.2013).
6. WASP [Электронный ресурс] // Новостной портал. Режим Доступа:http://airobot.ru 2013, http://airobot.ru/news/1972/ (Дата обращения: 13.05.2013).
7. Parrot AR.Drone 2 [Электронный ресурс] // официальный сайт. Режим Доступа:http://ardrone2.parrot.com/ (Дата обращения: 13.05.2013).
8. *AR.Drone API* [Электронный ресурс] // Блог. Режим Доступа:https://projects.ardrone.org/ (Дата обращения: 13.05.2013).
9. *PX4 Autopilot* [Электронный ресурс] // официальный сайт. Режим Доступа:https: // pixhawk.ethz.ch/px4/modules/px4ioar (Дата обращения: 13.05.2013).
10. *AIRCRACK-NG* [Электронный ресурс] // официальный сайт. Режим Доступа:http: //www.aircrack-ng.org/documentation.html (Дата обращения: 13.05.2013).
11. *GPUHASH* [Электронный ресурс] // официальный сайт. Режим Доступа: https://gpuhash.com/?menu=en-main (Дата обращения: 13.05.2013).
12. *Crazyflie Nano* [Электронный ресурс] // Интернет-журнал «Хакер». Режим Доступа: http://www.xakep.ru/post/60070/ (Дата обращения: 13.05.2013).

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Абрамов Евгений Сергеевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: abramoves@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Кобилев Максим Андреевич – e-mail: mkobilev@gmail.ru; кафедра безопасности информационных технологий; студент.

Abramov Evgeny Sergeevich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: abramoves@sfedu.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

Kobilev Maxim Andreevich – e-mail: mkobilev@gmail.ru; the department of security in data processing technologies; student.