ЛЕКЦИЯ 13. АТАКИ НА КВАДРОКОПТЕРЫ И ДРОНЫ

Беспилотный летательный аппарат (БПЛА, реже БЛА; в разговорной речи также «беспилотник» или «дрон», от англ. *drone* — трутень) — летательный аппарат без экипажа на борту.

БПЛА могут обладать разной степенью автономности — от управляемых дистанционно до полностью автоматических, а также различаться по конструкции, назначению и множеству других параметров. Управление БПЛА может осуществляться эпизодической подачей команд или непрерывно, в последнем случае БПЛА называют дистанционно-пилотируемым летательным аппаратом (ДПЛА).

Основным преимуществом БПЛА/ДПЛА является существенно меньшая стоимость их создания и эксплуатации (при условии равной эффективности выполнения поставленных задач) — по экспертным оценкам боевые БПЛА верхнего диапазона сложности стоят приблизительно $6 млн долл. США, в то время как стоимость сопоставимого пилотируемого истребителя составляет около 100 миллионов долларов.

Недостатком БПЛА является уязвимость систем дистанционного управления, что особенно важно для БПЛА военного назначения.

Классификация БПЛА по типу управления:

- управляемые автоматически;
- управляемые оператором с пункта управления (ДПЛА);
- гибридные.

Небольшие БПЛА используют литий-полимерные аккумуляторы.

13.1. Система связи и бортовая аппаратура управления БПЛА

В качестве бортовой аппаратуры управления, как правило, используются специализированные вычислители на базе цифровых сигнальных процессоров или компьютеры формата PC/104, MicroPC под управлением операционных систем реального времени (QNX, VME, VxWorks, XOberon). Программное обеспечение пишется обычно на языках высокого уровня, таких как Си, Си++, Модула-2, Оберон SA или Ада95.

Для передачи на пункт управления данных, полученных с бортовых сенсоров, в составе БПЛА имеется радиопередатчик, обеспечивающий радиосвязь с наземным приемным оборудованием. В зависимости от формата изображений и степени их сжатия пропускная способность цифровых радиолиний передачи данных с борта БПЛА может составлять единицы-сотни Мбит/с.

13.2. Технические недостатки ДПЛА

«Ахиллесовой пятой» БПЛА и особенно ДПЛА является уязвимость каналов связи — сигналы GPS навигаторов, как и любые сигналы, принимаемые и отсылаемые летательным аппаратом, можно глушить, перехватывать и подменять.

Для управления ДПЛА требуются каналы связи высокой пропускной способности, которые сложно организовать, особенно для загоризонтной (спутниковой) связи. Так, во время кампании США в Афганистане в распоряжении военных находились шесть «Предаторов» и два «Глобал Хоука», но одновременно в воздухе могли находиться лишь два и один БПЛА соответственно, а для экономии пропускной способности канала спутниковой связи пилоты были вынуждены отключать некоторые датчики и использовать видеопоток низкого качества.

В 2012 году учёными из Техасского университета в Остине была доказана практическая возможность взлома и перехвата управления БПЛА путём так называемого «GPS-спуфинга», но только для тех аппаратов, которые используют незашифрованный гражданский сигнал GPS.

Для стойкости к противодействию дрон обязан так или иначе иметь стойкость, сопоставимую с полноценными комплексами, что так или иначе повышает стоимость дрона и резко повышает риск массового уничтожения дронов минимальными средствами. Дрон зачастую ещё более тихоходен, маломанёвренен и зависим от помех, чем крылатая ракета.

Некоторые компании стали создавать защитные средства от дронов, позволяющие посадить аппарат или перехватить над ним управление. Понятно, что и производители дронов стараются как-то защитить свои устройства от перехвата. Но это далеко не всегда возможно, особенно, если за дело берутся настоящие эксперты своего дела. Ситуация усугубляется тем, что даже в самых продвинутых коптерах устанавливаются простейшие системы шифрования трафика.

13.3. Перехват дронов через DSMx

Команда исследователей создала систему, позволяющую перехватывать управление практически над любым дроном. Причём для этого не требуется электромагнитная пушка, разрешение властей или еще что-то. Достаточно использовать особым образом модифицированный пульт управления. Конкретно этот тип взлома позволяет перехватить управление любым коптером с протоколом передачи данных DSMx. Протокол используется не только для обмена данными с коптерами, он применяется и для работы с радиоуправляемыми автомобилями, катерами, вертолетами и т.п.

Технология не предполагает использование глушилки, блокирующей связь коптера с управляющим устройством. Вместо этого практикуется полный перехват управления с сохранением функциональность чужого дрона.

Для перехвата управления над чужим дроном используется атака по времени (timing attack), синхронизируя частоту излучателя своего пульта с частотой радиомодуля дрона в автоматическом режиме. После этого на дрон отправляется вредоносный пакет, который заставляет чужой аппарат игнорировать команды с «родного» котроллера, и начать слушать команды с контроллера злоумышленника.

Решить ситуацию с перехватом дронов сейчас нельзя — эта уязвимость актуальна для многих моделей радиоуправляемых устройств. Их производители не смогут быстро сменить протокол или тип радиоуправляемого модуля, который устанавливается в устройство. Решением может быть выпуск таких модулей, прошивку которых можно обновлять. Но это и дорого, и долго.

Специалисты также утверждают, что атаке по времени подвержены все современные радиоуправляемые системы. Для осуществления такой атаки нужно немного знаний об устройстве радиоуправляемых устройств и протоколов, которые используются для передачи данных по беспроводной сети, а также электронные компоненты на сумму примерно в $100. Интереснее всего то, что второй злоумышленник может использовать аналогичную систему для того, чтобы взломать первого, который, в свою очередь, перехватил управление над чьим-нибудь дроном.

13.4. Перехват дронов через Aircrack-ng

В 2013 году Сэми Камкар (Samy Kamkar) смог научиться управлять чужими дронами, сканируя радиочастоты при помощи своего дрона, на котором был установлен Raspberry Pi и приемопередатчик WiFi. Используемый метод взлома — Aircrack-ng.

При помощи этой утилиты специалист взламывал беспроводную сеть, а квадрокоптеры этой сети обнаруживались по особенностям их MAC-адреса. Как оказалось, коптеры такого типа имеют однотипные адреса, которые выделяют их среди всех прочих устройств.

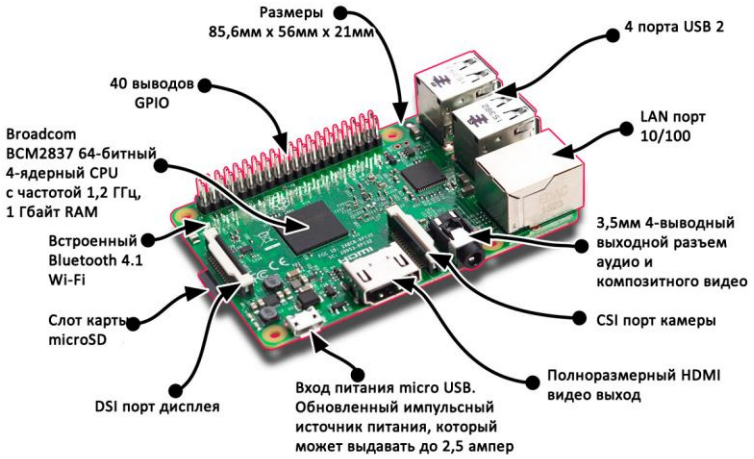
После взлома сети MAC-адреса WiFi сетей в зоне действия сигнала блокируются при помощи шпионского дрона, и чужие аппараты отключаются от родных контроллеров. После этого хакер получал возможность полноценного управления чужим коптером, а также получал изображение с их камер.

Схожий метод использовала группа специалистов по информационной безопасности shellntel. Она разработала надежную схему перехвата управлениями коптера. В этом методе используется эксплуатация уязвимости в протоколе телеметрии MAVlink. Такой протокол обычно передает данные в незашифрованном виде. Коптер и контроллер узнают друг друга по цифровому идентификатору. Специалисты собрали схему из миниатюрного компьютера Raspberry Pi и модуля радиосвязи, используя его в качестве сниффера.

Хакер Сэми Камкар (Samy Kamkar) разработал специального летающего дрона. Он ищет в воздухе поблизости другие дроны, взламывает их и передаёт контроль над ними самому хакеру. Дрон имеет название SkyJack и является модифицированной версией популярного радиоуправляемого квадрокоптера Parrot AR.Drone.

Работает конструкция от платы Raspberry Pi, небольшого аккумулятора и двух беспроводных передатчиков. SkyJack функционирует на специально разработанном программном обеспечении, через которое он автоматически ищет ближайшие дроны Parrot, взламывает их беспроводное соединение и передаёт управление над ними своему владельцу. SkyJack будет также взаимодействовать с устройствами, работающими на Linux, и взламывать все дроны в радиусе действия радиосигнала. На данный момент было продано 500 тысяч дронов Parrot начиная с их первой презентации в 2010 году. И все они могут быть захвачены с помощью одного SkyJack.

Raspberry Pi - Одноплатный компьютер размером с банковскую карту, изначально разработанный как бюджетная система для обучения информатике, впоследствии получивший намного более широкое применение и популярность, чем ожидали его авторы. Разрабатывается Raspberry Pi Foundation.



Aircrack-ng - это сетевой программный пакет, состоящий из детектора, пакетного анализатора, WEP и WPA/WPA2-PSK для взлома и анализатора для беспроводных локальных сетей 802.11. Он работает с любым контроллером беспроводного сетевого интерфейса, драйвер которого поддерживает режим необработанного мониторинга и может обнюхать трафик 802.11a, 802.11b и 802.11g. Программа работает под Linux, FreeBSD, OS X , OpenBSD и Windows; версия Linux упакована для OpenWrta также был перенесен на платформы Android, Zaurus PDA и Maemo; и доказательство порта концепции было сделано для iPhone.

Как оказалось, для перехвата управления беспилотником хватает отправки одного специально сформированного пакета. Изначально нужно перехватить идентификатор, а затем уже можно управлять функциями устройства. Специалисты утверждают, что в теории для коптеров, работающих с протоколом MAVLink можно задать GPS-координаты, и «пригонять» все устройства в одно место практически в автоматическом режиме.

13.5. Перехват дронов через Maldrone и Skyjack

Ещё один способ был предложен Рахулем Саси (Rahul Sasi). Он смог перехватить управление над такими устройствами, как Parrot AR.Drone 2.0 и DJI Phantom. Для достижения этой цели он использовал реверс-инжиниринг для проприетарного программного пакета AR Drone program.elf. В результате ему удалось успешно использовать комбинацию таких атак, как Maldrone и Skyjack. Саси утверждает, что его способ позволяет не только управлять чужими дронами, но и получать видеотрафик с их камер, как и в предыдущем случае.

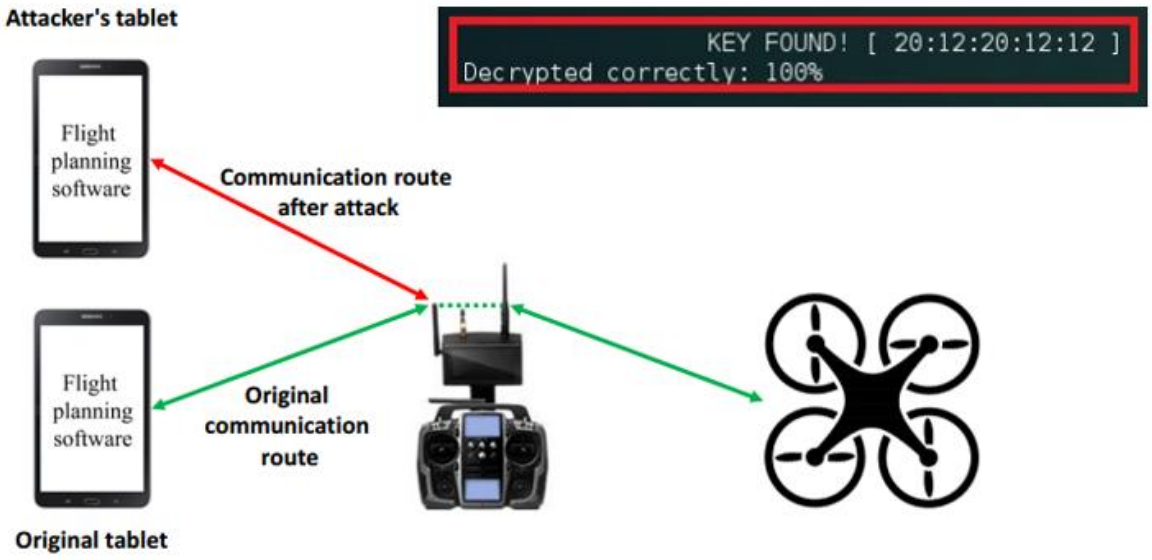
Проблемой этого способа является то, что сначала дрон полностью теряет управление, на несколько секунд, и начинает работать только после активации ПО, загруженного злоумышленником. Если дрон находится достаточно высоко, проблемы нет. Но если до земли всего несколько метров, аппарат может просто разбиться.

13.6. Перехват дронов через Wi-Fi

Практически универсальный способ взлома системы управления коптера показал Нильс Роддей (Nils Rodday) из IBM. На конференции Black Hat Asia он продемонстрировал, как взломать дорогой полицейский дрон, стоимость которых составляет десятки тысяч долларов США. А вот взломать такие устройства можно при помощи радиоэлектронной системы, стоимость которой — несколько десятков долларов.

В процессе взлома используется две уязвимости. Первая — это взлом беспроводной Wi-Fi сети. Обычно данные, принимаемые и передаваемые дроном, шифруются, но протокол шифрования в большинстве случаев — WEP. Его давно уже научились взламывать за доли секунды. Это простейшее шифрование, которое практически нигде уже не используется, но разработчики дронов решили внедрить именно такой протокол.

После взлома и подключения к сети злоумышленника им отправляется дрону команда, отключающая устройство от своей сети. После этого взломщик получает возможность управлять всеми функциями дрона.



13.7. Перехват дронов через на уязвимости чипов Xbee

Используется и другой тип взлома, основанный на уязвимости чипов Xbee. Они устанавливаются в большое количество различных моделей радиоуправляемых устройств. Шифрование данных чипом поддерживается, но во многих случаях разработчики его отключают. Именно поэтому злоумышленник может взломать дрон с таким чипом с расстояния нескольких километров.

Единственный способ защиты, по мнению автора такого способа взлома — использование шифрования данных.

13.8. Электронные пушки

Более простым способом воздействия на коптер является радиоэлектронная пушка. Компания Batelle создала уже несколько таких устройств. Наиболее эффективной можно назвать пушку DroneDefender. С ее помощью можно создать вокруг дрона зону радиомолчания. Пушка генерирует мощный радиосигнал, который обрывает подачу сигналов со стороны оператора. Кроме того, нарушается и позиционирование по GPS или ГЛОНАСС.

В этом году компания представила и «радиопистолет», который также создает мощные помехи по всему радиоспектру вокруг дрона. Отличием пистолета от DroneDefender является возможность определения типа сигнала, который передается дроном, с созданием помех лишь для используемой радиочастоты.

Пистолет может даже передавать команды, включая «домой» и «приземлиться». Команды подходят для большого количества моделей дронов.

13.9. Физическая нейтрализация дрона

Самым необычным способом нейтрализовать дрон, пожалуй, является «охота» на коптер с использованием другого коптера и сети. «Полицейский» коптер несет сеть, которую набрасывает на коптер-нарушитель. В случае удачного маневра нарушителя удается нейтрализовать.

Есть схожий метод, только здесь коптер несет пушку, заряженную сетью. Как только цель идентифицирована, полицейский коптер поднимается в воздух и стреляет сетью в нарушителя. Сеть при этом крепится к дрону-охраннику длинной и крепкой нитью, чтобы нарушитель, запутавшись в сети, не упал на землю и не разбился. Собранный «урожай» полицейский дрон уносит к месту посадки.

13.10. Система анти-дрон

Оборудование-локатор засекает приближающееся летательное устройство в радиусе 15 м с диапазоном фиксируемых рабочих частот от 1 МГц до 6,8 ГГц. По внешнему виду система больше всего напоминает большой Wi-Fi-роутер (взаимодействуют отдельные устройства Personal Drone Detection System между собой именно при помощи технологии Wi-Fi) и несколько условных «раций», каждая из которых и является тем самым датчиком обнаружения злобных жужжащих аппаратов. О приближении будет уведомление звуковым сигналом и отправка уведомления на заданное мобильное устройство.