В плохих руках он может обойти систему контроля доступа, помочь проникнуть в служебную зону или даже вскрыть автомобиль, а в хороших, так скажим, в руках специалиста по ИБ или разработчика - протестировать систему на безопасность и помочь в реализации своего проекта, в котором необходимо применение поддерживающего флиппером протокола. Это могут быть **NFC, RFID, iButton** и даже **радио-сигналы**, использующиеся в пультах удалённого доступа.

И перед тем, как мы приступим к сути статьи, я хочу показать один из примеров того, что может флиппер:

Выбираем чтение радио-сигналов:

Начинается сканирование:

Нажимаем на кнопки с пульта и видим, как флиппер перехватывает данные:

Выбираем любой из сигналов и транслируем его:

Вуаля! Мы взломали лампу и поменяли её цвет свечения через флиппер:

*ДИС****КЛЕЙ****МЕР:*

*Автор статьи никого не призывает к правонарушениям и отказывается нести ответственность за ваши действия. Вся информация предоставлена исключительно в ознакомительных целях. Спасибо!*

О поставках в Россию и заблокированном счёте разработчика:

К большому сожалению с недавних пор поставки в Россию закончились (будем надеяться, что временно).

Скорее всего, это связано с блокировкой счёта **PayPal**, на котором было **$1.3млн**. Об этом сообщил разработчик в своём **Twitter**:

По словам разработчика, в тех.поддержке **PayPal** сами не знают причин блокировки.

Прошивка, настройка и управление:

**Flipper Zero** - это проект Российского разработчика Павла Жовнера. Однажды он представил свою идею на кикстартере с целю заработать 60.000$ на разработку, но уже в первые сутки на счету был 1млн$, а итоговая собранная сумма составляет 4.8млн$.

С продажей флиппера на территории России возникло больше всего проблем из за огромного количества ограничений, но в последствии осуществить продажи всё же удалось, правда не надолго.

Недавно Павел поделился, что его счёт, на котором было более 1млн$ заблокировали без объяснений причин, вскоре после этого продажи вновь прекратились.

Начнём мы с того, что поставляется с кабелем **USB-Type C на USB**.

Кабель не простой и служит не только для зарядки, но и для передачи данных, а так как флиппер способен выполнять атаки типа **BadUSB** - это очень важно.

Уже из коробки флиппер умеет многое, но есть нюанс - функционал флиппера сильно урезан чтобы не противоречить законодательству, однако после покупки никто не запрещает сменить прошивку и разблокировать все функции. Собственно именно этим мы сейчас и займёмся.

Одна из самых популярных, да и функциональных на мой взгляд от **RogueMaster**, но список всех вы можете посмотреть на [этой странице](https://github.com/djsime1/awesome-flipperzero/blob/main/Firmwares.md):

Мы же рассмотрим установку именно от RogueMaster.

Сначала скачиваем и устанавливаем **qFlipper** на нашу ОС по этой ссылке:

<https://flipperzero.one/update>

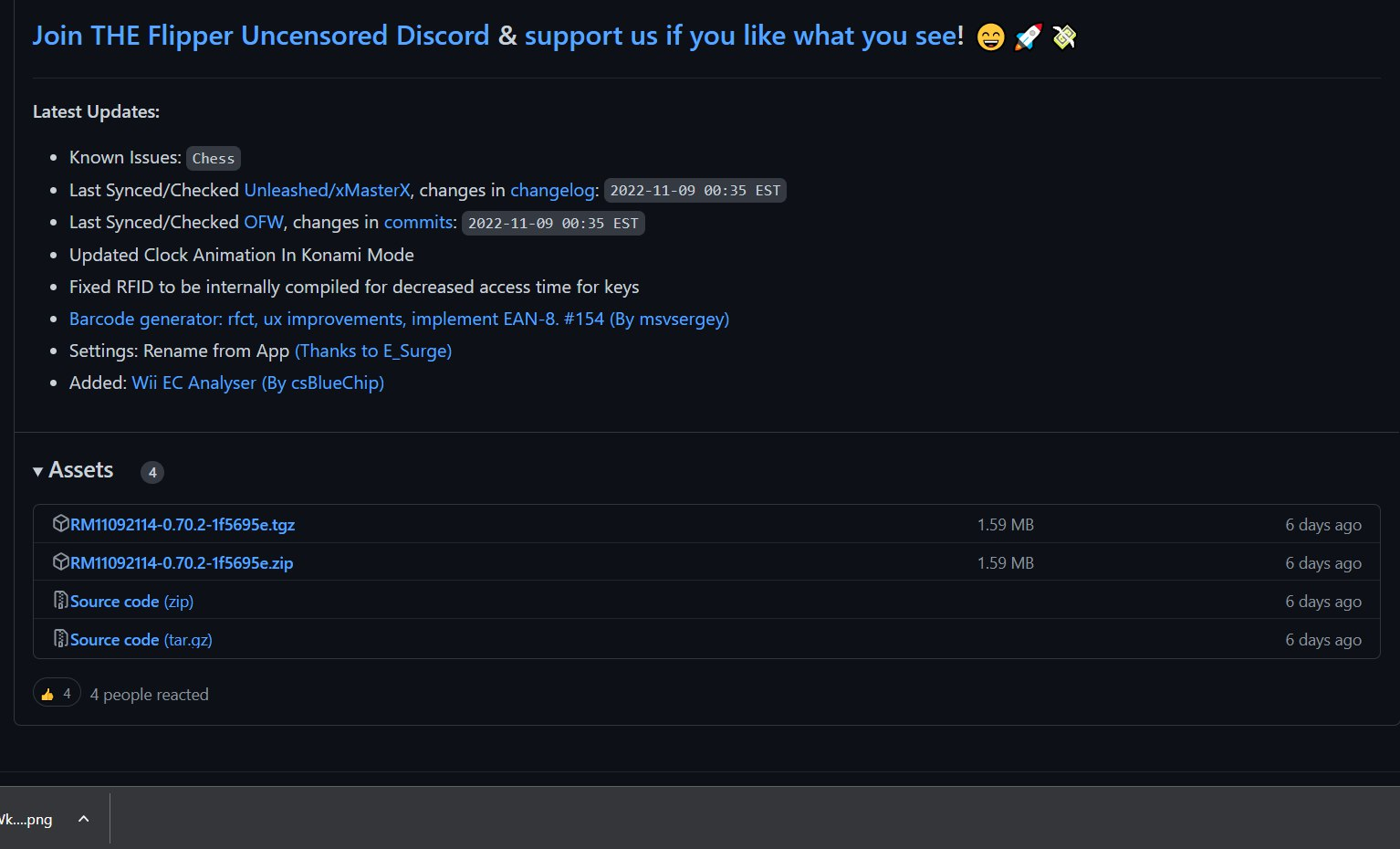
Далее вставляем SD-карту в устройство, подключаем его к компьютеру, открываем программу и обновляем прошивку нажатием на кнопку "**UPDATE**":

После этого полностью выключаем Flipper Zero (зажимаем кнопку "назад") и извлекаем из него SD-карту.

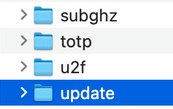
Вообще, есть 2 способа прошить флиппера. Первый, наиболее простой - через программу, а второй - вручную.

Мы воспользуемся именно вторым способом, т.к. автор прошивки заявляет, что он лучше.

Скачиваем самый свежий релиз по [этой ссылке](https://github.com/RogueMaster/flipperzero-firmware-wPlugins/releases) в виде zip-архива и распаковываем:



Теперь подключаем SD-карту к ПК, находим в ней папку «update» и помещаем в неё папку с файлами из скачанного архива:



В плохих руках он может обойти систему контроля доступа, помочь проникнуть в служебную зону или даже вскрыть автомобиль, а в хороших, так скажим, в руках специалиста по ИБ или разработчика - протестировать систему на безопасность и помочь в реализации своего проекта, в котором необходимо применение поддерживающего флиппером протокола. Это могут быть **NFC, RFID, iButton** и даже **радио-сигналы**, использующиеся в пультах удалённого доступа.

И перед тем, как мы приступим к сути статьи, я хочу показать один из примеров того, что может флиппер:

Выбираем чтение радио-сигналов:

Начинается сканирование:

Нажимаем на кнопки с пульта и видим, как флиппер перехватывает данные:

Выбираем любой из сигналов и транслируем его:

Вуаля! Мы взломали лампу и поменяли её цвет свечения через флиппер:

*ДИС****КЛЕЙ****МЕР:*

*Автор статьи никого не призывает к правонарушениям и отказывается нести ответственность за ваши действия. Вся информация предоставлена исключительно в ознакомительных целях. Спасибо!*

О поставках в Россию и заблокированном счёте разработчика:

К большому сожалению с недавних пор поставки в Россию закончились (будем надеяться, что временно).

Скорее всего, это связано с блокировкой счёта **PayPal**, на котором было **$1.3млн**. Об этом сообщил разработчик в своём **Twitter**:

По словам разработчика, в тех.поддержке **PayPal** сами не знают причин блокировки.

Прошивка, настройка и управление:

**Flipper Zero** - это проект Российского разработчика Павла Жовнера. Однажды он представил свою идею на кикстартере с целю заработать 60.000$ на разработку, но уже в первые сутки на счету был 1млн$, а итоговая собранная сумма составляет 4.8млн$.

С продажей флиппера на территории России возникло больше всего проблем из за огромного количества ограничений, но в последствии осуществить продажи всё же удалось, правда не надолго.

Недавно Павел поделился, что его счёт, на котором было более 1млн$ заблокировали без объяснений причин, вскоре после этого продажи вновь прекратились.

Начнём мы с того, что поставляется с кабелем **USB-Type C на USB**.

Кабель не простой и служит не только для зарядки, но и для передачи данных, а так как флиппер способен выполнять атаки типа **BadUSB** - это очень важно.

Уже из коробки флиппер умеет многое, но есть нюанс - функционал флиппера сильно урезан чтобы не противоречить законодательству, однако после покупки никто не запрещает сменить прошивку и разблокировать все функции. Собственно именно этим мы сейчас и займёмся.

Одна из самых популярных, да и функциональных на мой взгляд от **RogueMaster**, но список всех вы можете посмотреть на [этой странице](https://github.com/djsime1/awesome-flipperzero/blob/main/Firmwares.md):

Мы же рассмотрим установку именно от RogueMaster.

Сначала скачиваем и устанавливаем **qFlipper** на нашу ОС по этой ссылке:

<https://flipperzero.one/update>

Далее вставляем SD-карту в устройство, подключаем его к компьютеру, открываем программу и обновляем прошивку нажатием на кнопку "**UPDATE**":

После этого полностью выключаем Flipper Zero (зажимаем кнопку "назад") и извлекаем из него SD-карту.

Вообще, есть 2 способа прошить флиппера. Первый, наиболее простой - через программу, а второй - вручную.

Мы воспользуемся именно вторым способом, т.к. автор прошивки заявляет, что он лучше.

Скачиваем самый свежий релиз по [этой ссылке](https://github.com/RogueMaster/flipperzero-firmware-wPlugins/releases) в виде zip-архива и распаковываем:

Теперь подключаем SD-карту к ПК, находим в ней папку «update» и помещаем в неё папку с файлами из скачанного архива:

Вновь подключаем карту к флипперу и производим обновление. Для этого нажимаем кнопку "вниз", переходим к файловому браузеру, находим папку «update» и выбираем опцию «run in app»:



После успешного обновления вы получаете прошивку от RogueMaster, но это ещё не всё.

Теперь нам нужно убрать некоторые ограничения. Для этого мы вновь выключаем флиппер, извлекаем SD-карту и подключаем её к ПК, а далее переходим по пути **subghz > assets**.

В нём находим файл «**extend\_range.txt**» и устанавливаем параметр «ignore\_default\_tx\_region:» с false на **true** для игнорирования дефолтных региональных настроекSubGHZ:

Сохраняем изменения, вставляем SD-карту в устройство, включаем и пользуемся без ограничений!

Теперь об управлении:

Кнопка посередине из главного экрана откроет меню с выбором необходимого приложения. Там вы можете найти настройки, приложения для хакинга или перейти к играм.

Кратковременное нажатие кнопки "влево" на главном экране откроет часы, а длительное нажатие к файлам SubGHZ Remoute.

Кнопка "вниз" приведёт вас к файловому браузеру, а кнопка "вправо" к паспорту флиппера с отображением его уровня и настроения.

Максимум уровней вроде три, но прохождение всех трёх уровней никакого нового функционала не даёт. А чтобы эти уровни пройти - нужно просто перехватывать, транслировать и всякими другими образами взаимодействовать с радио-сигналами, NFC, RFID, ну и т.п. Короче чем больше данных вы собираете - тем счастливее флиппер.

Если вы застряли на режиме «**Games only**», который кстати говоря можно активировать в настройках, то выйти из него можно следующим образом:

Переходим к часам, нажав кнопку "влево", а далее нажимаем следующую комбинацию клавиш:

***ВВЕРХ***

***ВВЕРХ***

***ВНИЗ***

***ВНИЗ***

***ВЛЕВО***

***ВПРАВО***

***ВЛЕВО***

***ВПРАВО***

Таким же образом можно и включить режим «**Games Only**».

Менять анимацию главного экрана можно зажатием кнопки "ОК" посередине.

Помимо управления напрямую через кнопки, можно управлять флиппером через мобильное приложение по BlueTooth:

Или с компьютера по USB через программу qFlipper или по COM-порту через терминал.

Для первого способа нужно открыть программу и навести курсор на экран флиппера:

Далее нажать на этот экран и тогда откроется доступ к управлению:

Для второго способа нужно перейти к диспетчеру устройств и посмотреть занятый СОM-порт нашим устройством:

**Win+R**

devmgmt.msc

После этого переходим в программу PuTTy и указываем данные следующим образом:

Самая основная функция - **SubGHZ**, то есть перехват и трансляция радио-сигналов, что в свою очередь позволяет проверить возможность взлома собственного автомобиля, шлагбаума или чего-то ещё, что работает на дистанционном управлении по радио-сигналам.

Далее идут **RFID** и **NFC** для считывания данных с различных чипов и карт.

Флиппер может даже читать банковские карты, а с недавних пор ещё и чипы животных.

Кстати, банковские карты флиппер считывает с разными результатами. То есть флиппер может показать просто UID чипа, а может и номер карты с типом платёжной системы.

**iButton** - тоже очень интересный, но устаревший протокол, который используется для домофонных ключей и флиппер умеет с ним работать.

Ещё флиппер оснащён инфракрасным излучателем и приёмником для дистанционного управления телевизорами, кондиционерами и прочими устройствами.

Взлом Tesla:

На всех моделях Теслы используется специальный нешифрованный сигнал для открытия лючка зарядки. Чтобы когда подносишь «пистолет» зарядки к тесле — он автоматически открывается и добавляет больше поводов для выебончика в жизнь тесловода.

На прошивке от RogueMaster плейлист c кодами на Теслы вы можете найти в приложении **Sub-GHz Playlist** под названием "**example\_tesla.txt**":

Вновь подключаем карту к флипперу и производим обновление. Для этого нажимаем кнопку "вниз", переходим к файловому браузеру, находим папку «update» и выбираем опцию «run in app»:

После успешного обновления вы получаете прошивку от RogueMaster, но это ещё не всё.

Теперь нам нужно убрать некоторые ограничения. Для этого мы вновь выключаем флиппер, извлекаем SD-карту и подключаем её к ПК, а далее переходим по пути **subghz > assets**.

В нём находим файл «**extend\_range.txt**» и устанавливаем параметр «ignore\_default\_tx\_region:» с false на **true** для игнорирования дефолтных региональных настроекSubGHZ:

Сохраняем изменения, вставляем SD-карту в устройство, включаем и пользуемся без ограничений!

Теперь об управлении:

Кнопка посередине из главного экрана откроет меню с выбором необходимого приложения. Там вы можете найти настройки, приложения для хакинга или перейти к играм.

Кратковременное нажатие кнопки "влево" на главном экране откроет часы, а длительное нажатие к файлам SubGHZ Remoute.

Кнопка "вниз" приведёт вас к файловому браузеру, а кнопка "вправо" к паспорту флиппера с отображением его уровня и настроения.

Максимум уровней вроде три, но прохождение всех трёх уровней никакого нового функционала не даёт. А чтобы эти уровни пройти - нужно просто перехватывать, транслировать и всякими другими образами взаимодействовать с радио-сигналами, NFC, RFID, ну и т.п. Короче чем больше данных вы собираете - тем счастливее флиппер.

Если вы застряли на режиме «**Games only**», который кстати говоря можно активировать в настройках, то выйти из него можно следующим образом:

Переходим к часам, нажав кнопку "влево", а далее нажимаем следующую комбинацию клавиш:

***ВВЕРХ***

***ВВЕРХ***

***ВНИЗ***

***ВНИЗ***

***ВЛЕВО***

***ВПРАВО***

***ВЛЕВО***

***ВПРАВО***

Таким же образом можно и включить режим «**Games Only**».

Менять анимацию главного экрана можно зажатием кнопки "ОК" посередине.

Помимо управления напрямую через кнопки, можно управлять флиппером через мобильное приложение по BlueTooth:

Или с компьютера по USB через программу qFlipper или по COM-порту через терминал.

Для первого способа нужно открыть программу и навести курсор на экран флиппера:

Далее нажать на этот экран и тогда откроется доступ к управлению:

Для второго способа нужно перейти к диспетчеру устройств и посмотреть занятый СОM-порт нашим устройством:

**Win+R**

devmgmt.msc

После этого переходим в программу PuTTy и указываем данные следующим образом:

Самая основная функция - **SubGHZ**, то есть перехват и трансляция радио-сигналов, что в свою очередь позволяет проверить возможность взлома собственного автомобиля, шлагбаума или чего-то ещё, что работает на дистанционном управлении по радио-сигналам.

Далее идут **RFID** и **NFC** для считывания данных с различных чипов и карт.

Флиппер может даже читать банковские карты, а с недавних пор ещё и чипы животных.

Кстати, банковские карты флиппер считывает с разными результатами. То есть флиппер может показать просто UID чипа, а может и номер карты с типом платёжной системы.

**iButton** - тоже очень интересный, но устаревший протокол, который используется для домофонных ключей и флиппер умеет с ним работать.

Ещё флиппер оснащён инфракрасным излучателем и приёмником для дистанционного управления телевизорами, кондиционерами и прочими устройствами.

Взлом Tesla:

На всех моделях Теслы используется специальный нешифрованный сигнал для открытия лючка зарядки. Чтобы когда подносишь «пистолет» зарядки к тесле — он автоматически открывается и добавляет больше поводов для выебончика в жизнь тесловода.

На прошивке от RogueMaster плейлист c кодами на Теслы вы можете найти в приложении **Sub-GHz Playlist** под названием "**example\_tesla.txt**":