Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Цюрихские ученые обманули Keyless-Entry-Systeme | Les chercheurs de l'ETH ont trompé Keyless-Entry-System

Автор: Ольга Юркина, Цюрих , 08.07.2010.

Маленькой проволоки достаточно, чтобы взломать электронный код интеллектуальной системы безопасности (© ETH Zürich)

Сотрудники Швейцарской высшей технической школы Цюриха взломали машину своего начальника: в научных целях и по его собственной просьбе.

|

Les collaborateurs de l'ETH Zürich ont déchiffré le verrouillage à distance dans la voiture de leur chef: au nom de la science et sur sa propre demande.
Les chercheurs de l'ETH ont trompé Keyless-Entry-System

Оказывается, можно угнать машину и не только остаться безнаказанным, но и получить одобрение владельца: по крайней мере, Срдьян Тчапкун, профессор кафедры компьютерных технологий Высшей технической школы Цюриха (ETH), остался доволен работой своих сотрудников, которым он поручил взломать электронную систему бесключевого доступа своей машины. Орельен Франсийон и Борис Данев не только с легкостью справились с поставленной задачей и обманули модную систему Keyless-Entry, но и нашли хитроумные способы защиты от взломщиков электронных ключей. В опубликованном исследовании цюрихские ученые сначала рассказали о том, как взломать машину на электронной системе управления, а затем – как обезопасить себя от угонщиков.

Комфортабельная система бесключевого доступа, открывающая двери, словно по волшебству, в последнее время завоевывает все большую популярность среди автовладельцев. Компьютер, установленный в машине, реагирует на электронный чип, встроенный в ключ или смарт-карту владельца: достаточно приблизиться к автомобилю, как дверцы гостеприимно открываются, а мотор заводится легким нажатием на клавишу «Старт». Такой же удобной системой оснащена и новая машина профессора компьютерных технологий ETH Срдьяна Тчапкуна, и, так как глава исследовательской группы, занимающейся системами безопасности, отнюдь не равнодушен к беспроводным сетям и датчикам, он решил проверить, насколько можно доверять Keyless-Entry.


"Атака ретранслятора" в исполнении профессоров ETH (© ETH Zürich)
Тчапкун возложил на двух своих сотрудников важную миссию: попытаться угнать его собственную машину, прямо на стоянке университета. Орельен Франсийон и Борис Данев пришли от поручения в восторг и не заставили просить себя дважды. К их большому удивлению, хваленую беспроводную систему безопасности удалось раскусить при первых же попытках: профессора без труда оказались в чужой машине и даже смогли завести ее.

Дело в том, что для знатоков компьютерных технологий Keyless-Entry-System совершенно не отличается от других типов беспроводных сетей. Функционирование

электронного ключа обеспечивают расположенные в разных частях автомобиля антенны, посылающие кодовый сигнал, как только владелец приближается к машине. Специальный транспондер, встроенный в электронный ключ, расшифровывает сигнал и «отвечает» антеннам в автомобиле новым цифровым кодом. Автопилот машины сравнивает посланный и полученный сигналы и открывает доступ к машине и зажиганию, если коды совпадают.

«Таким образом, наша задача состояла в том, чтобы ввести систему машины в заблуждение, заставить ее поверить, будто транспондер ключа находится в непосредственной близости от нее. Хотя на самом деле он был в сумке удалившегося владельца», - объясняет Борис Данев. Взломщики во имя науки ожидали приближение своего коллеги в спортивном автомобиле на стоянке университета. Тчапкун закрыл машину, как подобает, и отправился работать на кафедру, спрятав электронный ключ в карман. На кафедре с ним столкнулся один из сообщников, в кармане которого было спрятано приемное устройство размером с MP3-плейер.

В это время второй «взломщик» стоял возле машины с передатчиком, связанным с антенной: «Роль антенны может выполнять обычная проволока», - выдает секрет Орельен Франсийон. Такая антенна, приставленная непосредственно к ручке двери, ловит сигнал, испускаемый антеннами машины и направляет его на передатчик, который трансформирует код и передает его на высокочастотных волнах приемному устройству в кармане второго сообщника. В свою очередь, приемное устройство передает сигнал на ключ в кармане у находящегося рядом владельца автомобиля. Ключ, само собой разумеется, отвечает на известный код. «Все происходит в одно мгновение, и вот машина уже открыта», - делятся впечатлениями профессора Франсийон и Данев. Найденный способ они проверили и на других моделях: результат оказался тем же, ведь все беспроводные ключи работают по одному и тому же принципу. Свой метод ученые назвали «атака ретранслятора»: основан он на том, что системе машины, в результате хитроумной игры с передатчиками, кажется, будто ключ владельца находится в непосредственной близости от нее.

У системы Keyless Entry тоже есть слабые места... (a1electric.com)
Однако цюрихские профессора разработали свой метод не для угонщиков, а для того, чтобы помочь автовладельцам обвести воров вокруг пальца. Элементарные меры безопасности позволяют обезопасить себя от подкованных в компьютерных технологиях воров. Первый способ: можно просто-напросто вынуть батарейки из беспроводного ключа на время своего отсутствия и открыть машину с помощью

запасного ключа, советуют цюрихские исследователи. «Это значительно усложняет угонщикам дело», - объясняют ученые, - «так как сначала им надо действительно взломать дверь машины». Побочное действие – беспроводная система теряет всякий смысл, и машина открывается с помощью обычного ключа.

Второй вариант – обернуть электронный ключ каким-нибудь металлом-непроводником, например, алюминиевой фольгой: она препятствует передаче беспроводного сигнала. Ворам пришлось бы значительно усилить сигнал, чтобы пробиться сквозь металлическую оболочку и получить ответ ключа и код машины. Однако самым удобным на данный момент является третий вариант защиты, разработанный Срдьяном Тчапкуном и его коллегой по System Security Group Каспером Бон Расмуссеном. С помощью их устройства, уже существующего в прототипе, возможно передавать антеннам автомобиля информацию о том, насколько в действительности удален от машины электронный ключ и встроенный в него транспондер: такая система не позволяет антеннам ошибаться и принимать сигналы от других устройств, то есть блокирует «атаку ретрансляторов».

Вот такой урок разработчикам интеллектуальных систем беспроводного доступа к машине преподнесли цюрихские ученые. Вполне возможно, что их противоугонные аксессуары будут пользоваться спросом. А автовладельцам и всем остальным остается посоветовать только одно: осторожнее обращаться с беспроводными новинками: никогда не знаешь, какой ретранслятор готовится поблизости к атаке.
ETH Zürich
Цюрих
Статьи по теме
С вулканами не шутят
Следующее авто Джеймс Бонд откроет с помощью часов
