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

Теория относительности в банкоматах | Théorie de la relativité aux bancomats

Author: Лейла Бабаева, Женева , 07.12.2021.

Прощайте, PIN-коды? © mrganso/pixabay.com

Ученые Женевского университета (UNIGE) и канадского Университета Макгилла разработали систему защиты банкоматов, используя знаменитую теорию Эйнштейна. Рассказываем, что у них получилось.

|

Des scientifiques de l'Université de Genève (UNIGE) et de l'Université McGill (Canada) ont développé un système de sécurité des bancomats utilisant la célèbre théorie d'Einstein. Voilà ce qu'ils ont fait.

Théorie de la relativité aux bancomats

Интересно, что несмотря на рост числа кибератак, швейцарцы не беспокоятся за сохранность своих данных – судя по их ответам в рамках исследования,

проведенного экспертами онлайн-платформы comparis, их позиция не изменилась по сравнению с 2020 годом. Доверие к системам оплаты в интернете даже выросло, в то время как в отношении постановлений в сфере защиты данных исследователи отметили определенный скептицизм.

А что, если действия хакеров однажды напугают население? На этот случай ученые уже подготовили решение, которое может заменить PIN-коды, используемые для снятия наличных в банкоматах. Исследователи обратились к проблеме трехцветной раскраски графа, который представляет собой математическую абстракцию реальной системы и включает в себя вершины (узлы) с парными связями, называемыми ребрами. Каждой вершине графа присваивается один из трех возможных цветов – желтый, синий или красный. Два узла, связанные ребрами, всегда должны быть разных цветов, поэтому если использовать большой граф, то подбор раскраски для него может стать серьезной математической задачей.

Как это связано с банкоматами? Каждому пользователю выдается устройство (токен) с уникальным графом и уже внесенным в память решением для раскраски. Цвета вершин графа регулярно меняются в соответствии с заданным алгоритмом. Пользователь подключает устройство к банкомату, последний отправляет сотни тысяч запросов и уточняет цвет отдельных вершин графа. Вся операция занимает около трех секунд. Благодаря готовому решению на токене проверка проходит успешно, при этом банкомат не получает полную раскраску всего графа, а только убеждается в ее непротиворечивости.

Такая система удобна тем, что даже если хакеры сумеют перехватить часть информации, им будет трудно восстановить полную раскраску для большого графа. В своем эксперименте ученые использовали граф с 5000 узлов и 10 000 ребер. Чтобы решить такую задачу, нужны огромные вычислительные мощности, а раскрасить граф путем простого перебора вариантов вряд ли получится быстро.

К чести исследователей стоит добавить, что такой уровень безопасности не вполне устраивал их в долгосрочной перспективе, так как функции кодирования, которые вычисляются в одном направлении, хотя и сложно декодировать, но не невозможно. Рассуждая таким образом, ученые решили усложнить процесс аутентификации и использовать два токена в двух банкоматах одновременно.

Сценарий происходящего напоминает ситуацию, когда полицейские допрашивают двух подозреваемых одновременно в разных комнатах. Если задержанные рассказывают одну и ту же версию истории, то существует вероятность, что они говорят правду. Используя этот принцип, можно проводить проверку сразу в двух банкоматах, в таком случае хакеру для перехвата учетной записи придется вычислить не один, а два больших графа за тот же промежуток времени. Чтобы исключить вероятность злонамеренного использования подключаемых к банкоматам токенов, ученые опирались на специальную теорию относительности, а конкретно на постулат о том, что мы не можем двигаться быстрее скорости света. Это распространяется и на скорость передачи данных. Таким образом, идея состоит в том, что задержки между запросами банкоматов и ответами пользовательских устройств всегда будут меньше, чем время для передачи информации на расстоянии между банкоматами. Можно сказать, что токены не успеют обсудить свои ответы между собой, чтобы их подделать.

Ученые испытали работу придуманной ими системы на расстоянии 390 м и 60 м между банкоматами. В будущем планируются сократить расстояние до одного метра. В настоящий момент главной проблемой является стоимость внедрения разработки. Для использования вышеописанной системы нужны очень мощные чипы, которые обойдутся недешево. Поначалу такую разработку могли бы применять крупные компании, которые готовы вложить средства в защиту своей ценной информации. Не исключено, что в будущем предложенное исследователями решение, основанное на работах гениального Эйнштейна, будет использоваться на предприятиях с повышенным уровнем безопасности: в банках, дата-центрах, в рамках важных инфраструктур.

[банки в Швейцарии]
Статьи по теме
[Банкоматы будущего теперь и в Швейцарии]
[Банкоматы в клочья]
[Microsoft создаст хранилища данных в Швейцарии]
[Берегите ваши данные!]
[Уже более ста лет в мире все относительно]
