ArtemyPrivet
20 дек 2020 в 21:58

Токен Авторизации

9 мин **75K**

Информационная безопасность*, Криптография*

Из песочницы

В настоящее время киберпреступность стала проблемой мирового уровня. Например, Дмитрий Самарцев, директор BI.ZONE в сфере кибербезопасности привёл на Всемирном экономическом форуме следующие цифры. В 2018 году ущерб мировой экономики от киберпреступности составил по его словам 1.5 триллиона долларов. В 2022 году прогнозируются потери уже в 8 триллионов, а в 2030 ущерб от киберпреступлений может превысить 90 триллионов долларов. Чтобы уменьшить потери от киберпреступлений, необходимо совершенствовать методы обеспечения безопасности пользователей. В настоящее время существует множество методов аутентификации и авторизации, которые помогают реализовать надежную стратегию безопасности. Среди них многие эксперты выделяют в качестве лучшей авторизацию на основе токенов.

До появления токена авторизации повсеместно использовалась система паролей и серверов. Сейчас эта система всё ещё остаётся актуальной из-за своей простоты и доступности. Используемые традиционные методы гарантируют пользователям возможность получить доступ к их данным в любое время. Это не всегда эффективно.

Рассмотрим эту систему. Как правило, идеология их применения базируется на следующих принципах:

1. Осуществляется генерация аккаунтов, т.е. люди придумывают сочетание букв, цифр или любых известных символов, которые станут логином и паролем.
2. Для осуществления возможности входа на сервер, пользователю требуется сохранять эту уникальную комбинацию и всегда иметь к ней доступ.
3. При необходимость заново подключиться к серверу и авторизироваться под своим аккаунтом, пользователю требуется заново вводить пароль и логин.

Кража паролей – это далеко не уникальное событие. Один из первых задокументированных подобных случаев произошел еще в 1962 году. Людям не просто запоминать разные комбинации символов, поэтому они часто записывают все свои пароли на бумаге, используют один и тот же вариант в нескольких местах, лишь слегка модифицируют с помощью добавления символов или изменением регистра некий старый пароль, чтобы использовать его в новом месте, из-за чего два пароля становятся крайне схожи. Логины по той же причине часто делаются одинаковые, идентичные.

Помимо опасности кражи данных и сложности с хранением информации, пароли также требуют проверки подлинности сервера, что увеличивает нагрузку на память. Каждый раз, когда пользователь входит в систему, компьютер создает запись транзакции.

Авторизация токенов – это система, работающая совершенно иначе. С помощью авторизации токенов вторичная служба проверяет запрос сервера. Когда проверка завершена, сервер выдает токен и отвечает на запрос. У пользователя все еще может быть один пароль для запоминания, но токен предлагает другую форму доступа, которую гораздо труднее украсть или преодолеть. И запись сеанса не занимает места на сервере. По сути токен авторизации - это устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца. Как правило, это физическое устройство, используемое для упрощения аутентификации.

Типы токенов авторизации

Токены авторизации различаются по типам. Рассмотрим их:

1. Устройства, которые необходимо подключить физически. Например: ключи, диски и тому подобные. Тот, кто когда-либо использовал USB-устройство или смарт-карту для входа в систему, сталкивался с подключенным токеном.
2. Устройства, которые находятся достаточно близко к серверу, чтобы установить с ним соединение, но оно не подключаются физически. Примером такого типа токенов может служить "magic ring" от компании Microsoft.
3. устройства, которые могут взаимодействовать с сервером на больших расстояниях.

Во всех трех случаях пользователь должен что-то сделать, чтобы запустить процесс. Например, ввести пароль или ответить на вопрос. Но даже когда эти шаги совершаются без ошибок, доступ без токена получить невозможно.

Процесс токен авторизации

Авторизация с помощью токена происходит следующим образом. Сначала человек запрашивает доступ к серверу или защищенному ресурсу. Запрос обычно включает в себя ввод логина и пароля. Затем сервер определяет, может ли пользователь получить доступ. После этого сервер взаимодействует с устройством: ключ, телефон, USB или что-то ещё. После проверки сервер выдает токен и отправляет пользователю. Токен находится в браузере, пока работа продолжается. Если пользователь попытается посетить другую часть сервера, токен опять связывается с ним. Доступ предоставляется или, наоборот, запрещается на основе выданного токена.

Администраторы устанавливают ограничения на токены. Можно разрешить одноразовый токен, который немедленно уничтожается, когда человек выходит из системы. Иногда устанавливается маркер на самоуничтожение в конце определенного периода времени.

Что такое аутентификация на основе токенов?

Аутентификация на основе токенов - это один из многих методов веб-аутентификации, используемых для обеспечения безопасности процесса проверки. Существует аутентификация по паролю, по биометрии. Хотя каждый метод аутентификации уникален, все методы можно разделить на 3 категории:

1. аутентификация по паролю (обычное запоминание комбинации символов)
2. аутентификация по биометрии (отпечаток пальца, сканирование сетчатки глаза, FaceID)
3. аутентификация токенов

Аутентификация токенов требует, чтобы пользователи получили сгенерированный компьютером код (или токен), прежде чем им будет предоставлен доступ в сеть. Аутентификация токенов обычно используется в сочетании с аутентификацией паролей для дополнительного уровня безопасности (двухфакторная аутентификация (2FA)). Если злоумышленник успешно реализует атаку грубой силы, чтобы получить пароль, ему придется обойти также уровень аутентификации токенов. Без доступа к токену получить доступ к сети становится труднее. Этот дополнительный уровень отпугивает злоумышленников и может спасти сети от потенциально катастрофических нарушений.

Как токены работают?

Во многих случаях токены создаются с помощью донглов или брелоков, которые генерируют новый токен аутентификации каждые 60 секунд в соответствии с заданным алгоритмом. Из-за мощности этих аппаратных устройств пользователи должны постоянно держать их в безопасности, чтобы они не попали в чужие руки. Таким образом, члены команды должны отказаться от своего ключа или брелока, если команда распадается.

Наиболее распространенные системы токенов содержат заголовок, полезную нагрузку и подпись. Заголовок состоит из типа полезной нагрузки, а также используемого алгоритма подписи. Полезная нагрузка содержит любые утверждения, относящиеся к пользователю. Подпись используется для доказательства того, что сообщение не подвергалось опасности при передаче. Эти три элемента работают вместе, чтобы создать высокоэффективную и безопасную систему аутентификации.

Хотя эти традиционные системы аутентификации токенов все еще действуют сегодня, увеличение количества смартфонов сделал аутентификацию на основе токенов проще, чем когда-либо. Смартфоны теперь могут быть дополнены, чтобы служить генераторами кодов, предоставляя конечным пользователям коды безопасности, необходимые для получения доступа к их сети в любой момент времени. В процессе входа в систему пользователи получают криптографически безопасный одноразовый код доступа, который ограничен по времени 30 или 60 секундами, в зависимости от настроек на стороне сервера. Эти мягкие токены генерируются либо приложением-аутентификатором на устройстве, либо отправляются по запросу через SMS.

Появление аутентификации на основе токенов смартфонов означает, что у большинства сотрудников уже есть оборудование для генерации кодов. В результате затраты на внедрение и

обучение персонала сведены к минимуму, что делает эту форму аутентификации на основе токенов удобным и экономически выгодным вариантом для многих компаний.

Безопасно ли использование токенов?

По мере роста киберпреступности и усложнение методов атак должны совершенствоваться методы и политика защиты. Из-за растущего использования атак “грубой силой”, перебора по словарю и фишинга для захвата учетных данных пользователей становится совершенно очевидно, что аутентификации по паролю уже недостаточно, чтобы противостоять злоумышленникам.

Аутентификация на основе токенов, когда она используется в тандеме с другими методами аутентификации, создает барьер 2FA, предназначенный для того, чтобы остановить даже самого продвинутого хакера. Поскольку токены могут быть получены только с устройства, которое их производит - будь то брелок или смартфон, системы авторизации токенов считаются очень безопасными и эффективными.

Но, несмотря на множество преимуществ, связанных с платформой токенов, всегда остается небольшой риск. Конечно, токены на базе смартфонов невероятно удобны в использовании, но смартфоны также представляют собой потенциальные уязвимости. Токены, отправленные в виде текстов, более рискованны, потому что их можно перехватить во время передачи. Как и в случае с другими аппаратными устройствами, смартфоны также могут быть потеряны или украдены и оказаться в руках злоумышленников.

Рекомендации по аутентификации на основе токенов

Реализация надежной стратегии аутентификации имеет решающее значение, когда речь идет о том, чтобы помочь клиентам защитить свои сети от нарушения безопасности. Но для того, чтобы стратегия действительно была эффективной, требуется выполнение нескольких важных основных условий:

1. Правильный веб-токен. Хотя существует целый ряд веб-токенов, ни один из них не может обеспечить ту же надежность, которую предоставляет веб-токен JSON (JWT). JWT считается открытым стандартом (RFC 7519) для передачи конфиденциальной информации между несколькими сторонами. Обмен информацией осуществляется цифровой подписью с использованием алгоритма или сопряжения открытого и закрытого ключей для обеспечения оптимальной безопасности.
2. Приватность.
3. Использование HTTPS-соединений. HTTPS-соединения были построены с использованием протоколов безопасности, включающих шифрование и сертификаты безопасности, предназначенные для защиты конфиденциальных данных. Важно использовать HTTPS-соединение, а не HTTP или любой другой протокол соединения при отправке токенов, так как эти в ином случае возрастает риск перехвата со стороны злоумышленника.

Что такое JSON веб-токены?

JSON Web Token (JWT) - это открытый стандарт (RFC 7519), который определяет компактный и автономный способ безопасной передачи информации между сторонами в виде объекта JSON. Эта информация может быть подтверждена благодаря цифровой подписи. JWT может быть подписан с помощью секрета (с помощью алгоритма HMAC) или иным образом, например, по схемам RSA или ECDSA.

В своей компактной форме веб-токены JSON состоят из трех частей, разделенных точками: заголовок, полезная нагрузка, подпись. Поэтому JWT выглядит обычно выглядит следующим образом: «xxxx.yyyy.zzzz».

Заголовок состоит из двух частей: типа токена, которым является JWT, и используемого алгоритма подписи, такого как HMAC SHA256 или RSA.

Вторая часть токена - это полезная нагрузка, содержащая информацию о пользователе и необходимые дополнительные данные. Такая информация бывает зарегистрированной, публичной и частной.

Зарегистрированная - это набор ключей, который не является обязательными, но рекомендуются для обеспечения улучшения безопасности. Например, iss - уникальный идентификатор стороны, генерирующей токен, exp - время в формате Unix Time, определяющее момент, когда токен станет не валидным, и другие.

Публичная информация может быть определена по желанию теми, кто использует JWT. Но они должны быть определены в реестре веб-токенов IANA JSON или определены как URI, который содержит устойчивое к коллизиям пространство имен. Частная - это пользовательская информация, созданная для обмена данными между сторонами, которые согласны их использовать. Получим вторую часть с помощью кодирования Base64Url.

Тоже не понял, что за прикол там происходит.

Подпись же используется для проверки того, что сообщение не было изменено по пути, а в случае токенов, подписанных закрытым ключом, она также может подтвердить, что отправитель JWT тот, за себя выдает.

Выходные данные представляют собой три строки Base64-URL, разделенные точками, которые могут быть легко переданы в средах HTML и HTTP, будучи при этом более компактными по сравнению со стандартами на основе XML, такими как SAML.

Пример:

```
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NSIsIm5hbWUiOiJKb2huIEdvbGQiLCJhZG1pbiI
```

К плюсам использования JWT можно отнести размер - токены в этом языке кода крошечные и могут быть переданы между двумя пользователями довольно быстро; простоту - токены могут быть сгенерированы практически из любого места, и их не нужно проверять на сервере; контроль - можно указать, к чему пользователь может получить доступ, как долго будет длиться это разрешение и что он может делать во время входа в систему.

К минусам стоит отнести всего один ключ - JWT полагается на один ключ, из-за чего вся система окажется под угрозой в случае, если он будет скомпрометирован; сложность - JWT токены не так просто понять, из-за чего, разработчик, не обладающий глубокими знаниями алгоритмов криптографической подписи, может непреднамеренно поставить систему под угрозу; ограничения - нет возможности отправлять сообщения всем клиентам, и невозможно управлять клиентами со стороны сервера.

Почему стоит использовать токены авторизации?

Многие люди считают, что если текущая стратегия работает хорошо (пусть и с некоторыми ошибками), то нет смысла что-то менять. Но токены авторизации могут принести множество выгод.

Они хороши для администраторов систем, которые часто предоставляют временный доступ, т.е. база пользователей колеблется в зависимости от даты, времени или особого события. Многократное предоставление и отмена доступа создаёт серьёзную нагрузку на людей.

Токены авторизации позволяют обеспечить детальный доступ, т.е. сервер предоставляет доступ на основе определенных свойств документа, а не свойств пользователя. Традиционная система логинов и паролей не допускает такой тонкой настройки деталей.

Токены авторизации могут обеспечить повышенную безопасность. Сервер содержит конфиденциальные документы, которые могут нанести компании или стране серьезный ущерб при выпуске. Простой пароль не может обеспечить достаточную защиту.

Есть и другие преимущества использования этой технологии. Но даже уже перечисленных достаточно, чтобы внедрить её на сервера.

Теги: токен, авторизациия, аутентификация

Хабы: Информационная безопасность, Криптография

Карма Рейтинг

@ArtemyPrivet

Пользователь

Комментарии 8

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

tigreavecdesailes
8 часов назад

Выжимаем ATtiny10, практическое применение

Средний 10 мин 2.5K

Из песочницы Сезон DIY

+31 15 24

DiTsi
12 часов назад

Установка для засветки фоторезиста при производстве печатных плат

Средний 4 мин 2.9K

Кейс Сезон DIY

+31 29 28

iliazeus
6 часов назад

Внутреннее представление и оптимизации строк в JavaScript-движке V8: «отмываем» строки, «обгоняем» C++

Средний 8 мин 1.5K

Обзор

+30 16 0

Edemit
вчера в 18:32

Я выучил иностранный язык за год и у вас тоже получится

Простой · 7 мин · 18K

Туториал

+29 · 167 · 165

NatalieVT
6 часов назад

Встречаем ТВ Станции — новые устройства, которые объединяют технологии телевизоров и умных колонок

13 мин · 2.8K

+25 · 11 · 30

Ekamelev
14 часов назад

125 простых советов по улучшению юзабилити вашего сайта

22 мин · 1.8K

Перевод

+22 · 56 · 6

Agastos_sec
8 часов назад

Отечественные платформы виртуализации и их безопасность

11 мин · 1.5K

+21 · 21 · 3

kira_kalimulina
5 часов назад

Дорогая, что-то пошло не так. Гид по пустым состояниям и ошибкам + шаблоны на все случаи

Простой · 11 мин · 1.1K

Аналитика

+19 · 13 · 5

nckma

8 часов назад

Моя марбл машина, версия 3

3 мин 2.1K

Сезон DIY

+17 7 19

klimensky
7 часов назад

Прошлое и настоящее глубоководных погружений

18 мин 2.6K

+15 14 9

Боль, лень и продакты: как вытащить идею из молчаливого новичка

Турбо

Показать еще

МИНУТОЧКУ ВНИМАНИЯ

Забился на крутые ивенты в Календаре на Хабре

Эврика: цены падают из-за Промокодуса!

ЗАКАЗЫ

Настроить передачу конверсий из трекера Binom через FB Conversion API

1100 руб./за проект · 2 отклика · 25 просмотров

Создать бота для покупки токенов в сети Binance Smart Chain

30000 руб./за проект · 19 откликов · 92 просмотра

Настройка переадресаций на outlook почте

3000 руб./за проект · 4 отклика · 26 просмотров

Сверстать 2 страницы по figma

2000 руб./за проект · 25 откликов · 72 просмотра

Разработка мобильного приложения на Android и iOS

70000 руб./за проект · 15 откликов · 44 просмотра

Больше заказов на Хабр Фрилансе

ЧИТАЮТ СЕЙЧАС

upd: Пользователи по всей России жалуются на массовый сбой в работе VPN-протоколов OpenVPN и WireGuard

48K 169

Google построила для сотрудников отель с номерами по $99 за ночь

3.2K 14

Мы живем в компьютерной симуляции. Мнение программиста. Часть 1

1.6K 10

Bleeding-edge обход блокировок с полной маскировкой: настраиваем сервер и клиент XRay с XTLS-Reality быстро и просто

61K 212

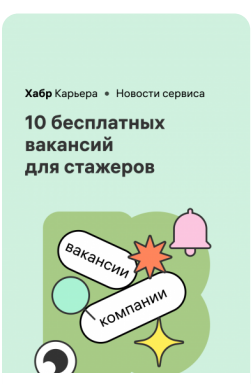
Я выучил иностранный язык за год и у вас тоже получится

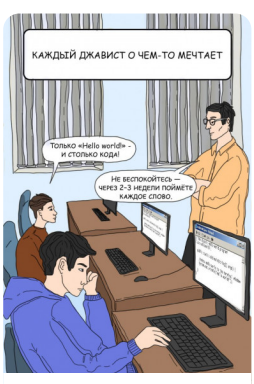
18K 165

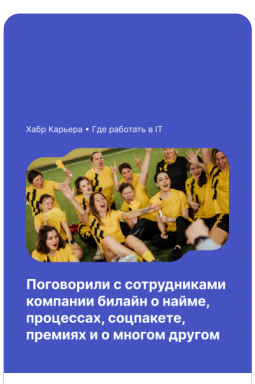
Боль, лень и продакты: как вытащить идею из молчаливого новичка

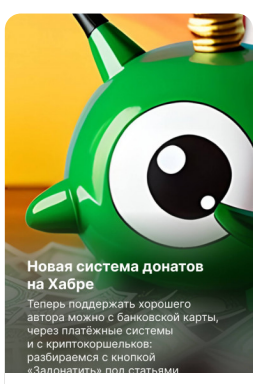
Турбо

ИСТОРИИ









Дарим вакансии для стажеров

О чём мечтают джависты

Лучшие статьи из блогов компаний

Где работать в IT: билайн

Новая система донатов на Хабре

Что почи сезоне D

РАБОТА

Специалист по информационной безопасности
117 вакансий

Все вакансии