«надежная защита в условиях полностью враждебного окружения»

Конфиденциальность
Анонимность
Безопасность

SSG Web Portal

https://secserv.me

«Доверяйте математике. Криптография Ваш друг.» Брюс Шнаер

Описание

Электронная переписка, в которой вместо открытого текста используются URL ссылки на зашифрованное сообщение либо файл.

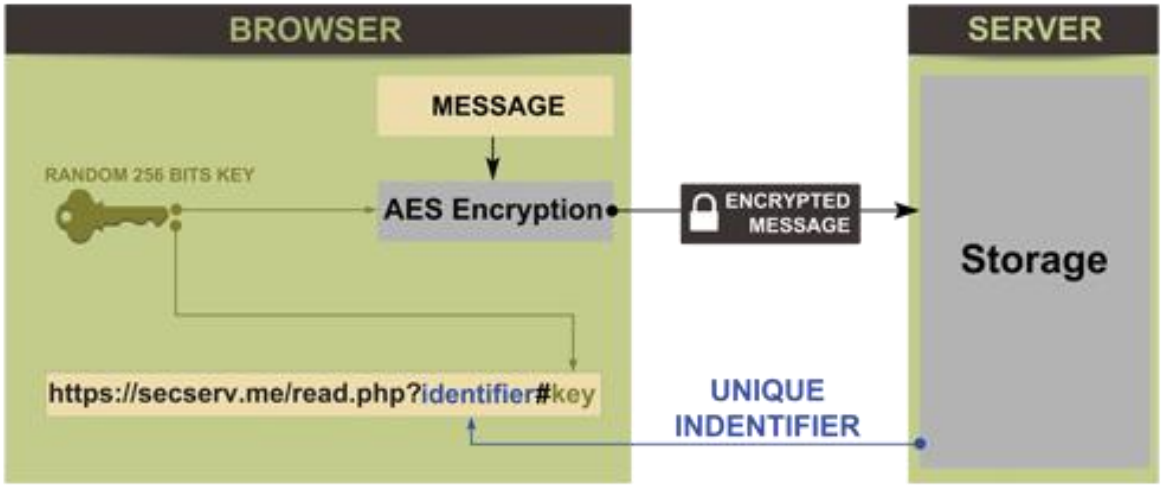
Для примера, вот URL сообщение которое сгенерировано на сайте https://secserv.me :

https://logdog.pw/?mYxCTvrPbTuJD7iWkVWj#4ItJjJVenLTZFhXSJH1Ej881YEghHT9pXSQ_aqDuzly+FnsA2Q33uBlyuzZLRTSY Здесь первая часть mYxCTvrPbTuJD7iWkVWj — это идентификатор сообщение, который отправляется на сервер, а вторая часть 4ItJjJVenLTZFhXSJH1Ej881YEghHT9pXSQ_aqDuzly+FnsA2Q33uBlyuzZLRTSY используется для дешифровки и на сервер не отправляется.

В ссылке передается ключ шифрования, который не получает сервер – чем гарантируется конфиденциальность передачи данных. Сервер не имеет возможности анализировать получаемую информацию, что обусловлено тем что ключ находится в той части URL которая не передается на сервер.

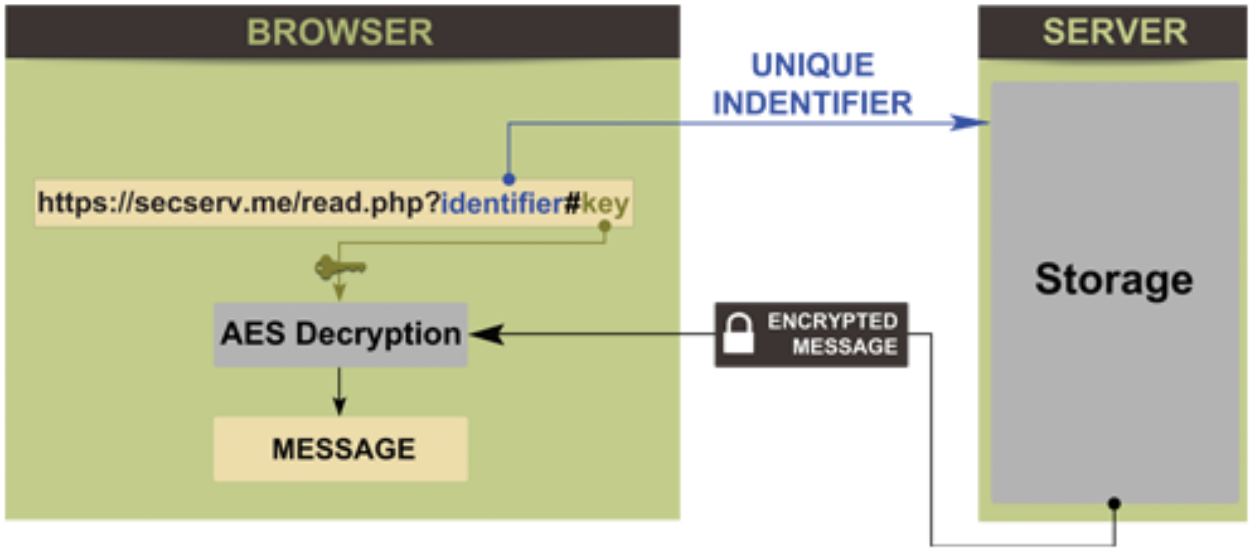
При повторном открытии URL пользователь видит такое : https://logdog.pw/?что-угодно-пишите-так-как-сервер-не-знает-есть-ли-такой-айди))

Формула.Создание сообщения



- Пользователь вводит сообщение и делает запрос на создание ссылки на это сообщение.
- Клиент (браузер) создает случайный ключ для симметричного шифрования. Ключ - это очень большое число, подобрать которое, при современном уровне техники не представляется возможным.
- Клиент шифрует сообщение с помощью ключа и отправляет зашифрованное сообщение на сервер (но не отправляет ключ).
- Сервер получает сообщение, назначает ему случайный номер и отсылает этот номер клиенту. Номер - это тоже очень большое число.
- На основании номера сообщения и ключа, клиент создает ссылку на сообщение.

Формула.Чтение сообщения



- Отправитель отправляет адресату не само сообщение, а ссылку, которая содержит номер сообщения и ключ шифрования.
- Клиент адресата по номеру сообщения делает запрос к серверу и получает зашифрованное сообщение. Клиент не отправляет ключ. Сервер удаляет сообщение.
- Клиент расшифровывает сообщение с помощью ключа.
- Wuala! Пользователь читает сообщение.

Формы

1.Передача текстового сообщения и файла. https://secserv.me/

We will encrypt it and create Link to it for you:

https://logdog.pw/?PcBV+9VWzJdoe1093Pi4#447mY3m2lY6QAd29wYhey7nkB1mloY7t5+FOtPW9C8yb_5_+opA9UfR2sFiFe60b

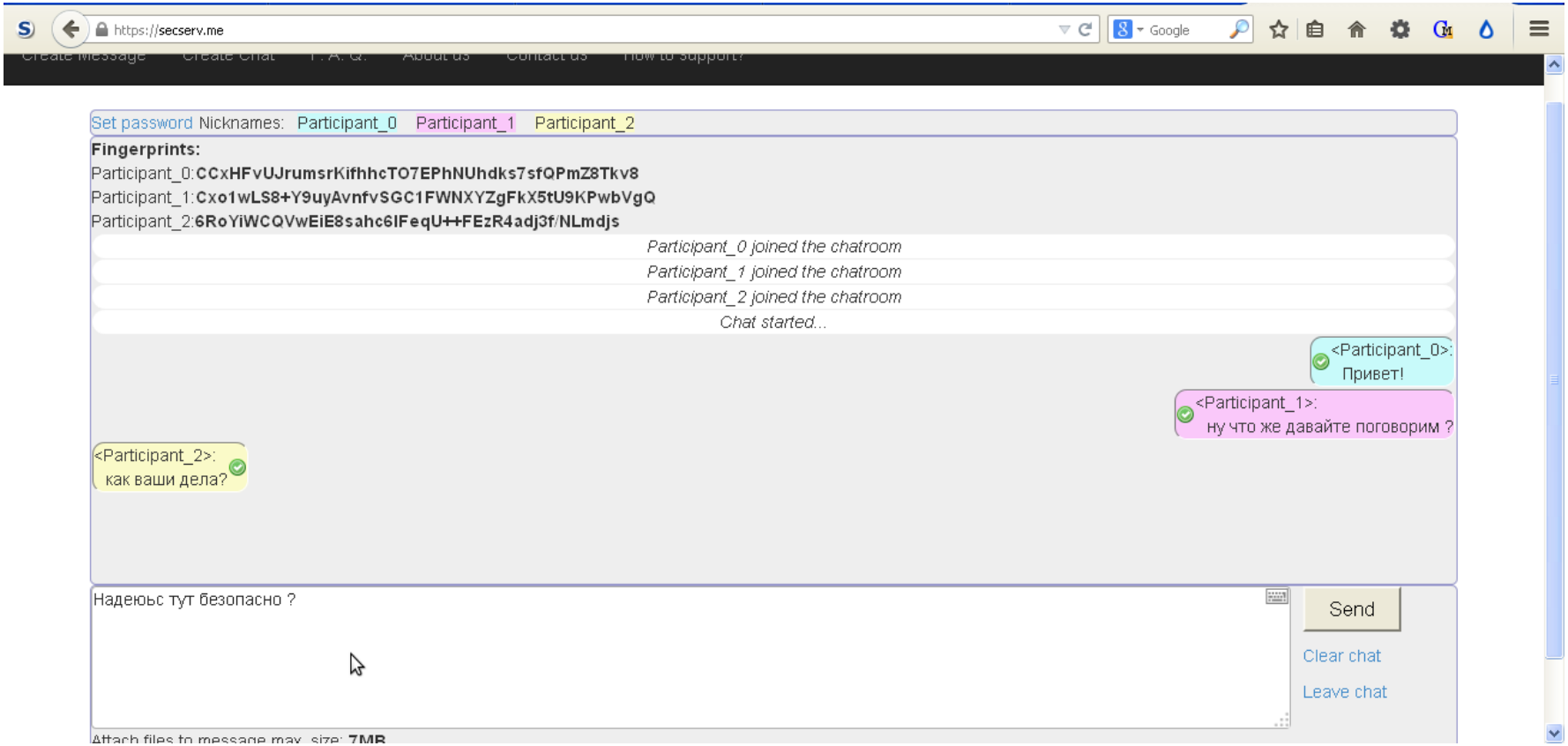
Show QR Code

Send this link instead of real message to your friend for additional security.

See why we cannot read your message for details.

You are fully responsible for your message content

2.Передача текстовых сообщений и файлов в форме веб-чата https://secserv.me/#create_chat



Основная целевая аудитория сервиса

Юристы

Финансисты

Службы безопасности

Бизнесмены

Преимущества. Зачем нужен общий секрет - фраза-пароль?

Проблема может возникнуть, если злоумышленник сможет полностью прослушать канал связи, по которому передается ссылка, а так же заполучить зашифрованное сообщение.
В этом случае может помочь только общий секрет - пароль. При использовании пароля, перед расшифровкой сообщения, на ключ накладывается преобразования, которое зависит от пароля, а для шифрования/дешифрования используется преобразованный ключ.

Таким образом, даже перехватив весь поток данных, зашифрованное сообщение, злоумышленник не сможет прочитать сообщение.

Используя фразу-пароль клиент не нуждается в HTTPS шифровании обмена данными с сайтом

Восстановить сообщение по прочитанным ссылкам невозможно в принципе.

Преимущества. Зачем нужен random pool?

Создание случайных ключей - это узкое место криптографии. Случайный ключ создается с помощью генератора случайных чисел. Очень важно иметь хороший генератор, чтобы он не был предсказуемым, иначе, ключ возможно будет подобрать.

Ходят слухи, что Агентство Национальной Безопасности США сделало всё, что могло, чтобы внедрить слабые генераторы случайных чисел, чтобы иметь возможность подбирать ключи шифрования.

Домыслы это или нет, сказать сложно, но мы сделали всё, чтобы не зависеть от существующих генераторов, мы добавили "случайность", которая зависит от того, как пользователь двигает мышкой, нажимает на клавиши и пр.

Качество технической реализации этой идеи, всегда может изучить грамотный специалист.

Преимущества

- В случае несанкционированного доступа к каналу связи (e-mail, skype, viber etc.), злоумышленник увидит просто набор неработающих ссылок.

- Нет необходимости доверять хранилищу данных на сервере, т.к. сервер получает сообщения в зашифрованном виде, но никогда не получает ключа. В мире недобросовестной конкуренции, не всегда можно доверять общедоступным хранилищам данных.

- Пользователь всегда может "отозвать" отосланное сообщение, просто прочитав его - оно удалиться автоматически.

- Возможность защитить сообщение от перехвата с помощью общего секрета и добавить файл до 7MB как вложение. Безопасная и анонимная альтернатива «мониторящим» почтовым сервисам.

- Открытость. Технически грамотный пользователь может проверить данную схему работы.

Применение

Ситуация	Не используя https://secserv.me	Используя https://secserv.me
Общение через социальные сети, почту и чаты	При взломе сервисов вся информация достается злоумышленнику	При взломе сервисов злоумышленник видит только прочитанные ссылки, которые не работают
Общение информаторов/юристов/полиции	Возможна компрометация переписки, если под давлением злоумышленники завладевают телефоном/ноутбуком клиента	НЕ возможна компрометация переписки, если под давлением злоумышленники завладевают телефоном/ноутбуком клиента, так как может быть использована ссылка с 2 паролями. Также в любой момент Вы можете закрыть вкладку с чатом или сообщением. Пример: Перейдите со ссылке https://logdog.pw/?7mgR9y, в поле Enter passphrase введите пароль 22222222 - прочтите ложное сообщение, теперь удалите пароль в поле Enter passphrase кнопкой Backspace, снова введите пароль в поле Enter passphrase но 1111 – прочтите правильное сообщение.

Дополнительная опция

- Дополнение функционала сервиса и внедрение виртуальной клавиатуры для защиты от троянов на ПК

СПАСИБО ЗА ВНИМАНИЕ!