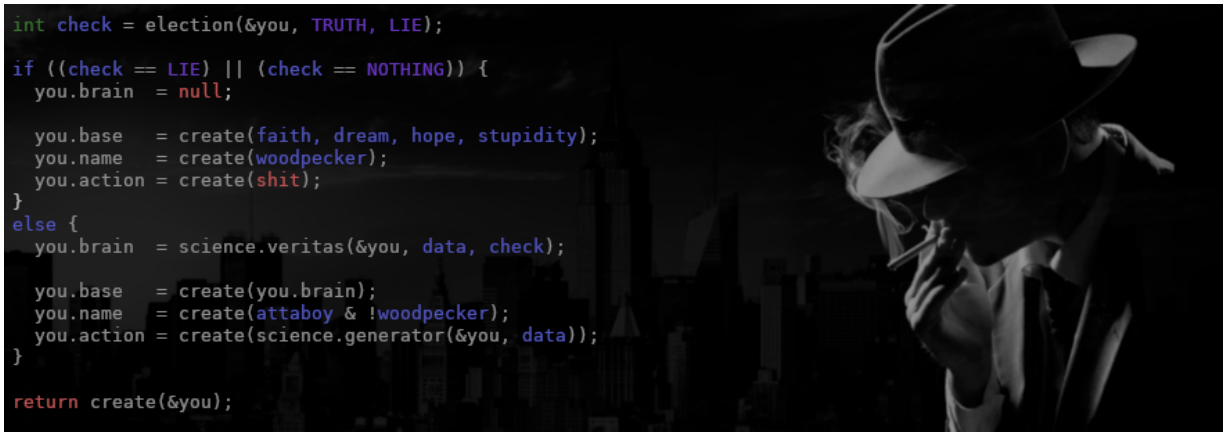
Наука и вера в лучший мир

Статьи, 14 июля в 14:49 ARR0III



Привет читатель. Я хочу рассказать тебе то, что я недавно понял, когда у меня наконец дошли руки до правки кода разработанной мной программы для шифрования файлов. Скажу прямо, программа посредственная и умного в ней мало (нет даже механизма проверки подлинности шифротекста), но это лучшее что я делал, и эта программа служит мне верой и правдой вот уже не один год, защищая мой парольный файл вида [https://site.domain | password | secret].

Я использовал в своей программе только свободный код, проверенные десятилетиями шифры и хэши, зарекомендовавшие себя способы организации взаимодействия частей программы (стереть из памяти пароль сразу после превращения его в ключ, исключить стековые буферы и т.д), тестировал программу так, насколько хватило ума, и в конце концов остался доволен как слон. Но, когда я дошел до анализа путей утечек информации, ахнул.

Как оказалось, все мы в полной [цензура]. И это не шутка.

Когда вы используете программное обеспечение для защиты своих секретов, как и любое другое программное обеспечение, вы верите в лучший мир. Сейчас я расскажу, что

такое вера в лучший мир, и почему это страшно.

Представим что вы купили компьютер в магазине, запустили интернет браузер Mozilla Firefox или любой другой, ввели пароль на своем любимом сайте, где безопасно общались всё это время и передали сообщение Алисе. Спустя 4 дня, вам пришло письмо со спамом, в котором вам предлагают купить то, что вы обсуждали с Алисой. Вы в шоке, а Алиса в слезах, так как ей тоже пришел спам, из текста которого следует, что ваш секрет уже и не секрет вовсе, а анекдот, рассказываемый сотрудниками ближайшего рекламного агентства. Как же рекламное агентство узнало ваш секрет? Вы ведь были защищены вашим компьютером, операционной системой, интернет браузером, сайтом и уверены в том, что Алиса никому и ничего не говорила. Были защищены? Нет, это вера в лучший мир.

Вы верите в то, что у производителя вашего компьютера есть совесть, и что он, опьяненный многомиллиардной прибылью от продажи данных пользователей, не наплевал на закон. В то, что он не последний [цензура], который (к примеру) встроил в контроллер жесткого диска чип с плохой реализацией хорошего шифра Rijndael, в которой каждый чётный бит ключа шифрования всегда равен 1.

Вы верите в то, что разработчики операционной системы, честные и неподкупные люди, которые готовы из кожи вон вылезти, лишь бы защитить вашу информацию, а значит и вас. В то, что ребята из проекта (к примеру) Linux, не тролли-злодеи, что модифицировали пару строчек в ядре ОС так, чтобы ослабить шифрование раздела подкачки, потому что «Да кто вообще будет это ломать?».

Ваша вера в то, что создатели сайта, на котором вы общаетесь с Алисой, люди хорошие, добрые, не торгуют вашими секретами со всеми у кого есть деньги, и конечно же они никогда не насмехаются над вами, когда читают ваши сообщения, мешает вам и Алисе хранить тайны. Вы верите в то, что программы для общения, безопасны настолько,

насколько их рекламируют их же производители. Ведь это [название сайта], они дорожат своей репутацией! Нет.

> У нас в России, как и в мире вообще, как говорят некоторые учёные, «Репутационная катастрофа» — ты никто и звать тебя никак, даже если ты доктор наук и дважды академик.

Вы верите в то, что мир справедлив, добр, и вообще вон те парни из [страна/корпорация] отличные ребята!

```
<sarcasm>Они умные, честные и знают своё дело!</sarcams>
```

Вы верите в то, что на вас не смотрят как на букажку сотрудники специальных служб, которые просто ради смеха могут использовать ваши фотографии в качестве валюты у себя на работе, обсуждая за бутылкой пива складки на вашем животе или родимые пятна на спине. Как же так? Ведь это же [страна/служба], они демократы, честные ребята! Хм… Я бы хотел жить с такой верой — меньше стресса.

Из чего идет такая вера?

Нам, людям, нужен простой, легко объясняемый, в первую очередь нами же самим себе, черно-белый мир, где всё понятно, просто и по хорошему, но мир не такой.

Вы верите в то, что все эти люди, как и многие другие из их начальников и подчиненных, само воплощение честности на земле, день и ночь работающие на благо человечества, а их программы, чудо инженерной мысли. Нет, это не так, что подтверждается наблюдениями:

> Наш мир, очень опасное и коварное место, где водятся волшебные драконы с острыми клыками, огромными кошельками, сильным аппетитом, приобретенным слабоумием и отсутствием совести.

Вы верите в то, что все элементы информационной цепи,

имеют такой же запас прочности, как элемент цепи, контролируемый вами, что наивно, так как вы не контролируете все элементы. И никогда не будете. Никогда.

Скажу прямо: я был невероятно слеп, когда начинал разработку программы.

Ах да, и конечно же вы верите в то, что язык Алисы находится за зубами и не распространяет ваши интимные секреты ради поднятия настроения коллег в курилке, просто по глупости.

Вы верите в то, что математики, работающие под контролем и на деньги государств, не дурачат вас, когда представляют миру новый, уникальный, неповторимый алгоритм шифрования. Но, научная честность бесценна! Ученый, создавший уязвимый алгоритм шифрования, и молчавший об этом ради торжества демократии и защиты свободного мира, будет очень долго объясняться, как это так: *ему было известно что алгоритм уязвим более 20 лет, а он никому за эти годы не сказал?* Люди, спроектировавшие поточные шифры GEA-1 и GEA-2 для защиты сотовой связи, умышленно ослабили его, и скоро им придется давать объяснения: *почему уязвимость миллиардов людей ничто по сравнению с гипотетической гибелью десятков?*

Ученые каждый день приходят к новым, качественным умозаключениям, и большинство из ученых невозможно подкупить, так как «абсолют истины» нерушим, а репутация, зарабатываемая десятилетиями, слишком дорога, чтобы терять ее ради денег. Это значит, что сколько бы не скрывали данные о нашем мире, всё равно рано или поздно, найдется смельчак, который заявит:

```
if (a == 2) then b = 198473552.0951;
```

В науке лгать просто бесполезно, так как науки изучают мир, а мир изучаем всеми и всегда. Рано или поздно истина всё равно всплывет в работе какого нибудь выскочки, и тогда придется оправдываться за необъяснимое молчание. Но и это вера в лучший мир, так как мы верим в то, что большинство

исследователей не ошиблись, вовремя заметили аномалию, или просто не дурачат нас, потому что им так веселей живется. Над дураками смеялись всегда, а ученые такие же люди как и все те, кто насмехался над невеждами 200, 300, 500 лет назад. Разница лишь в том, что ученые редко обманывают, всегда признают что ошибались и в отличие от всех остальных, работают над тем, чтобы сегодня люди были немножко умнее чем вчера.

Если никто из вас не ученый-информатик, как и я, то остается только верить в то, что нас не дурачат те, кому мы слепо доверяем. Правительств это тоже касается, потому что от правительств зависит почти всё, и именно правительства решают, что пускать на внутренний рынок а что блокировать. Одураченный верой в лучший мир и ослепленный налогами политик, пришедший к решению впустить в страну уязвимый шифр, только потому что его придумали учёные, ни чем не лучше человека, впустившего лису в курятник только потому что у лисы оказалась при себе бумажка, похожая на ветеринарный пропуск.

> Глупость всегда хуже злонамеренности, потому что глупость нельзя исправить, в ней нет выгоды и злых планов «Доктора Смерть», а значит ее труднее заметить, и конечно же за нее не наказывают.

Если уж и верить в лучший мир, то только в такой, где факт и расчет имеют высший приоритет, а не маркетинговые заявления вроде: *Наш продукт отвечает всем международным стандартам качества и зарекомендовал себя на рынке; Защита мирового уровня по семейным ценам; Всё для безопасности вашей семьи — в одном продукте;*

— Простите, а AR-15 и бронежилеты в комплекте? Кто нибудь может сказать что это вообще значит и как оно попало в мозг человека, который не постыдился это ляпнуть?

Представьте что вам нужно пройти по минному полю, и вам

предлагают металлоискатель фирмы [название фирмы] очень напоминающий старую русскую тяпку. Продавец рассуждает о магнитных полях, давлении взрывных газов при взрыве в тонн/см2, собственном военном опыте и т.д. Если он будет достаточно уверен в себе, вы будете подавлены его психологической жесткостью, уверенностью в собственной правоте и с высокой долей вероятности купитесь на его рассказы. Вам будет просто неловко задавать ему вопросы, так как вы будете бояться показать себя человеком непонимающим, глупым, невежественным, занудным и т.д. Кстати именно так и работает подавление свободы личности в армиях, тоталитарных сектах и других группах, где нужно переломить хребет человеческой воли и подчинить себе желания других людей.

Но, вас с такой же высокой долей вероятности ждет смерть от взрыва, так как:

> Слова ничего не стоят, покажите мне код.

Да и вообще, тяпка не пищит при контакте с металлами. К тому же, продавец разумеется не расскажет о том, что он несколько раз был судим, его штрафовали за нарушение антимонопольного законодательства, и вообще человек он мягко скажем, так себе. Его клиенты каждый день подрываются на том же минном поле, а он сам при проходе через то же минное поле не использует никакие тяпки, а использует карту минного поля, которую ему любезно продали на местной военной базе за 10 тыс. руб. Да, он тот еще молчун…

В примере выше очевидно, что тяпку вам предлагает обычный мошенник, который просто хочет денег, но в мире компьютерных технологий, почти никто такого не замечает. И не должен, так как не ученый-информатик. К тому же, тяпку вы не получите, так как это интеллектуальная собственность производителя, а если и получите, то в аренду, и вообще не

факт что это на самом деле тяпка — железяка на палке просто так выглядит.

> Вера в лучший мир опасна для жизни, потому что при ней у нас не может возникнуть стимула к улучшению ситуации, в которой мы находимся, и тем более у нас нет стимула проверить, всё ли в порядке. Мы гибнем, и не догадываемся об этом.

Ведь мы думаем: Этот шифр уж точно никто не взломает; Эта ОС используется в NASA. Серьезно? Никто? NASA? Вы видите будущее и уверены в том, что в NASA не верят в лучший мир? Вера в лучший мир дает нам чувство того, что мы в относительной безопасности, в то же время, мы не думаем о том, что обманываем себя успокаивающими надеждами. Нам просто неприятно думать о себе как о людях, которые уязвимы, больны, необъективны, наивны, глупы — близки к выходу из зоны душевного спокойствия. Мы избегаем таких мыслей, потому что нам от них больно, и в этом наша ошибка, чем во все времена пользовались люди, чуть хитрее нас. Кто это такие? Мошенники! Шарлатаны! Лжецы! Продавцы ложных надежд, как никто другой понимающие, что даже с учетом вреда полученного нами от веры в их сказки, мы получим и пользу.

Да, именно так. И они правы. В чем польза от обмана для того, кого обманули? Даже если обманутый и гибнет, поверив в сказку, то гибнет в меньшем стрессе и со спокойным сердцем. Мы умираем с верой. Верой в то, что всё обязательно будет хорошо. Разве не этого всегда хотел человек, чтобы всё обязательно было хорошо? Спросите врачей, они подтвердят, насколько это важно, внушить больному, что впереди всё будет хорошо, рядом будут любимые, хорошие люди, и мы обязательно будем счастливы. Надежда хорошо выступает духовным обезболивающим, но это самообман, ведущий к гибели.

Брюс Шнайер, американский математик и криптограф, уже очень давно написал знаменитую статью «Ханаанский бальзам», в которой ясно изложил, как технологические компании дурят людей, эксплуатируя их непонимание того, как же на самом деле работают системы защиты информации. Эта статья очень хорошо, на примерах разъясняет читателю, как его дурят ради выгоды и к прочтению обязательна каждому, кто хочет знать, чего стоит опасаться при взаимодействии с торговцами Wunderwissenschaft (нем. Чудо-наука).

Что же мне делать? Куда бежать, кому звонить, в какой колокол бить кувалдой? Ответ: *просто продолжать верить в то, что другие программисты сохранили совесть и не стали троллями-злодеями*. Вот так, просто верить в лучшее и слепо доверять, так как ничего больше просто невозможно предпринять, иначе придется стать «доктором около-всяческих наук». Таким образом, не боясь каждого техника, сохранить психическое здоровье и надеяться на ученых-разоблачителей. Оправдана ли такая надежда? Не знаю, склонен думать что нет.

Простите, если был груб. Я просто посчитал себя обязанным рассказать самое важное, к чему пришел на пути защиты собственных секретов.

Скажу прямо: прекратите верить в сказки о том что мы живем в розово-сиреневом мире, где детские игрушки из под кровати, поют нам колыбельные. Кроме вас, ваша безопасность нужна только вашим родным, и то не всегда.

С учетом вышесказанного, я избрал для себя следующую стратегию защиты данных:

- Использовать только одобренные свободным сообществом и зарекомендовавшие себя годами операционные системы, программы и протоколы, такие как Debian, TAILS, Whonix, Tor, GnuPG, XMPP.
- Компьютер не должен иметь жесткого диска, или жесткий

диск должен быть отключен от материнской платы на уровне аппаратуры, во избежание сохранения незащищенных данных на материальном носителе.
- При работе с критичными данными, компьютер должен быть лишен связи с внешним миром на аппаратном уровне.
- Операционная система, работающая на компьютере, должна быть только в виде LiveUSB.
- Любое средство беспроводной связи — шпионское устройство и главный свидетель.
- У любого сервера есть собственник, скованный законами и соглашениями (Telegram, VK, Twitter, Google и т.д.) — осторожнее с ними, потому что они не друзья.
- Защита информации такая же часть военной науки, как и вооруженная оборона городов.
- Вера — понятие религиозное.
- Рыба попадается на крючок только тогда, когда открывает рот.
- **Никто не должен знать то, чего знать не обязан.**

И последнее:

> **Государства никогда не используют средства защиты информации, не изготовленные под их прямым контролем. Это просто запрещено!**