XYO Network (Сеть XYO):
Риски безопасности и способы их снижения

Arie Trouw* (Ари Трау), Andrew Rangel (Эндрю Ренджел), Jack Cable (Джек Кейбл)

Февраль 2018 года

---

1 Введение

Сеть XYO – это не нуждающаяся в доверии децентрализованная криптографическая геолокационная сеть, которая использует доказательства с нулевым разглашением для установления высокой степени достоверности в проверке местоположения. Основной проблемой для сети XYO, как и для всех децентрализованных и не нуждающихся в доверии объектов, является безопасность системы. К уязвимостям относятся, но не ограничиваются: недостатки проектирования/архитектуры, ошибки кода, некорректная экономическая мотивация и социальная инженерия. Основное внимание в данном документе обращено на недостатки проектирования/архитектуры и экономическую мотивацию.

---

2 Технические особенности

2.1 Резюме

В данном документе рассматриваются концепции высокого уровня в отношении потенциальных атак на сеть XYO. В связи с тем, что сеть использует не нуждающуюся в доверии систему, предполагается, что все участники сети уязвимы (например, стражи, мосты и т.д.). В данном разделе описываются некоторые известные атаки на уровне протокола, а также стандартные меры защиты от них. Все остальные атаки предполагают, что устройства в системе скомпрометированы.

---

*XYO Network, **arie.trouw@xyo.network**

2.2 Bluetooth

В большинстве Bluetooth-устройств используется настройка сопряжения «ключ долговременного пользования», которая устанавливает PIN-код, используемый для шифрования. Если ключ обнаруживается путем перехвата процесса сопряжения, весь будущий трафик может быть легко дешифрован. Существуют инструменты, которые могут подобрать PIN-код методом грубой силы. Даже надежно отработанные схемы, которые устанавливают пароль вне протокола, обычно выполняются в незашифрованном виде. Это открывает двери для нескольких типов атак, целью которых является получение доступа к протоколу. Кроме того, устройства можно легко заполучить, ускорив таким образом эти подходы.

Для того, чтобы предотвратить атаки такого типа, MAC-адреса из белого списка могут воспрепятствовать взаимодействию неавторизованных устройств со стражами и мостами. Еще один способ противостоять этим атакам – требовать от пользователя физического нажатия кнопки «сброс» для того, чтобы привязать устройство, что предотвратит атаки пользователей, у которых нет прямого физического доступа к устройству.

2.3 Обновления по воздуху (OTA)

Стражам необходима возможность выполнять обновления «по воздуху» (OTA). Обновления OTA позволяют выполнять быстрые исправления для улучшения стабильности и безопасности устройства. Недостатком этой функции является возможность атаки, которая подменяет это обновление и добавляет вредоносный код.

2.3 Аппаратные средства

Устройства в сети XYO физически разбросаны по самым разным местам по всему миру. Это означает, что существует постоянная возможность для физического компрометирования устройства. Это главная причина, по которой сеть XYO не нуждается в доверии. Вся система опирается на сложные алгоритмы, которые тщательно и усердно анализируют историю и содержание данных, поступающих в систему. Любые данные, которые не получили высокую оценку и не являются длинно-цепочными, не учитываются, а устройства-нарушители наказываются.

3 Атак «Poison the Well»

3.1 Резюме

Атака «Poison the Well» происходит тогда, когда неисправный или вредоносный субъект создает и вводит поврежденные данные, что снижает общую точность и/или достоверность результатов, генерируемых системой.

3.2 Мотивация

Цель злоумышленника в атаке «Poison the Well» состоит в том, чтобы разрушить или испортить данные, которые отправляются определенному стражу или мосту. Это позволит им вызвать как краткосрочное, так и долгосрочное экономическое потрясение. Учитывая, что сеть XYO является не нуждающейся в доверии системой, для такого типа данных установлен низкий допуск в систему.

Хотя злоумышленник и не получит прямой выгоды от таких действий, он получает выгоду от нарушения и/или подделки репутации данных других людей. Предположим, что сеть XYO использовалась для отслеживания местонахождения лиц, находящихся на условно-досрочном освобождении, с тем чтобы сообщить о любых нарушениях условий условно-досрочного освобождения. Если бы она использовалась для учета количества времени, которое серийный нарушитель правил, запрещающих вождение в нетрезвом виде, проводит на баре, нарушитель условий условно-досрочного освобождения может «отравить колодец», отправляя плохие данные на мост бара, пока тот не будет отсоединен от сети. Нарушитель может затем нарушить условия своего условно-досрочного освобождения и употреблять алкоголь в баре столько, сколько ему или ей хочется. Даже если предоставленные данные сообщают, что преступник находится в районе бара, отравленные данные могут уменьшить достоверность до такой степени, что они окажутся недействительными.

3.3 Технический анализ

На геолокационные данные стража могут повлиять GPS-глушилки или незаконные радиочастотные передатчики, которые предназначены для вмешательства в авторизованную радиосвязь. Устройства GPS-спуфинга [1] могут отправлять ложные данные на GPS-радиоприемники, чтобы фальсифицировать местоположение.

Стражи, сообщающиеся через Bluetooth, представляют собой еще один вектор для этого типа атаки. Существуют различные способы, в которых устройство Bluetooth может быть спровоцировано на отправку плохих данных [2]. Хотя секретные ключи, создаваемые сетью XYO, немедленно удаляются, остается возможность того, что устройство может подслушать сообщение между стражем и мостом и скопировать отправленные данные. Этот вор сможет тогда отправить плохие данные, притворившись стражем, и начать отравлять данные, которые мост посылает архивариусам.

3.4 Меры протокола по снижению рисков

Активную GPS-глушилку можно легко распознать из-за загрязнения, которое она оказывает на общую область, на которую нацелена. Например, любой пользователь сотового телефона в области работы глушилки может столкнуться с внезапным блокированием многих приложений, которые он использует. Это лишь вопрос времени, когда несколько сторон подтвердят подобные проблемы и смогут подтвердить, что виновником является глушилка. Учитывая, что этот тип сбоев легко фиксируется, в сочетании с тем фактом, что FCC ясно постановил, что вызывающие помехи устройства являются незаконными [5], высокий риск, связанный с этим типом атаки, делает вероятность ее возникновения низкой. Тем не менее, существуют сложные методы анти-спуфинга GPS, которые в настоящее время разрабатываются как на уровне аппаратных средств, так и на уровне программного обеспечения для дополнительной безопасности [1].

В дополнение к этим мерам безопасности, существуют современные технологии и стратегии, которые позволяют нам организовать защиту от Bluetooth-спуфинга и сбоев, такие как аутентификация ключей связи защищенными соединениями. [3]

3.5 Меры сети XYO по снижению рисков

Сеть архивариуса – это конкурентная сеть, которая возвращает проверенные данные, запрашивемые провидцами. В момент, когда архивариусы получают данные (подробно описывается в желтом документе), сеть начинает отсекать плохие данные. Передача информации, хранящейся в цепочке обратно источнику, позволяет обнаруживать недавно добавленные плохие данные, даже с подделанной информацией в длинной цепочке. Каждый архивариус также перекрестно проверяет данные других архивариусов, чтобы построить обоснованный консенсус для сети. Из-за того, что архивариусы вместе с мостами и стражами получают плату, внутренняя криптоэкономика подавляет попытки отравить компоненты нижнего уровня.

3.6 Заключение

Учитывая, что архивариус получает данные из широкого географического региона, и для того, чтобы отравить этот регион, нужно найти его физическое местоположение, такой тип атаки приведет к тому, что злоумышленник будет наказан сетью. Именно это лишает злоумышленника экономических стимулов для проведения такой атаки на сеть XYO.

4 Атака «Assassination»

4.1 Резюме

Атака «Assassination» происходит тогда, когда злоумышленник пытается дискредитировать узел (убийство персонажа) или сделать другой узел нефункциональным (техническое убийство).

4.2 Мотивация

В атаке «Assassination» злоумышленник мотивирован подорвать репутацию легитимных узлов, чтобы повысить относительную достоверность других узлов, контролируемых злоумышленником. Поскольку репутация стражей в сети XYO имеет основополагающее значение для функционирующей сети, крайне важно обеспечить, чтобы репутацией узлов нельзя было легко манипулировать.

Рассмотрим ситуацию, в которой злоумышленник пытается транслировать ложную информацию о местоположении в сети XYO (подробнее описывается в атаке типа «Force Field»). В этом случае злоумышленник должен сначала нацелиться на отдельные узлы, чтобы нанести вред их репутации. Один из способов, которым это может быть достигнуто – это выборочное подписывание, когда злоумышленник выборочно предоставляет ложную информацию легитимному стражу (делая его данные сильно отклоняющимися от нормы), чтобы сделать узел менее согласованным с другими узлами в сети XYO. Это приводит к снижению репутации стража по сравнению с другими узлами сети.

Кроме того, злоумышленник может предпринять техническое убийство узла, например, физически уничтожив устройство. Эти типы атак также предпринимаются в попытках сфальсифицировать информацию о местоположении в сети и приводят к неисправности устройств.

4.3 Технический анализ

Атака «Assassination» на стража требует, чтобы злоумышленник развернул как минимум одно устройство для избирательного общения со стражем-целью. Поскольку другие устройства в сети не генерируют подписи с вредоносным узлом, вредоносный узел отображается только на узле-цели.

Для мостов, не входящих в сеть, информация, передаваемая узлом-целью, является несовместимой с остальной частью сети. Это приводит к тому, что узел-цель теряет репутацию в остальной сети, которая продолжает не распознавать вредоносный узел.

4.4 Меры протокола по снижению рисков

Основополагающим для защиты от атаки «Assassination» является установление наказания для репутации узла, если он участвует в избирательном подписывании. В этом случае вредоносные узлы участвуют в избирательном подписывании, чтобы сделать себя невидимыми для других стражей в сети.

Установление репутации каждого стража в соответствии с его согласованностью с остальной частью сети позволяет наказывать узлы, которые участвуют в избирательном подписывании. Узел с хорошей репутацией может выдавать запрос на менее авторитетный узел в сети. Если менее авторитетный узел является легитимным, в его интересах было бы подписать запрос и сделать его видимым для сети, повысив свою репутацию. Таким образом, если узел будет практиковать выборочное подписывание, более авторитетный узел может транслировать то, что вредоносный узел отказался подписывать свой запрос. Эта практика не может быть использована в случае, когда узел фактически подписывает запрос, поскольку легитимный узел может затем транслировать свою подпись, чтобы опровергнуть обвинение в выборочном подписывании.

Наказывание избирательного подписывания в сети XYO снижает риск атак «Assassination» на персонажей, поскольку у каждого стража имеется защитный механизм против получения противоречивой информации.

4.5 Меры сети XYO по снижению рисков

Создание репутации для каждого стража препятствует узлам участвовать в избирательном подписывании. Это снижает риски атаки «Assassination» на персонажей, подвергая каждого стража в сети наказанию за избирательное подписывание. Физические атаки типа «Assassination» (например, уничтожение устройства) сложнее предотвратить на сетевом уровне, но сеть XYO устойчива для атак, нацеленных на отдельные устройства.

4.6 Заключение

Создание системы репутации позволяет стражам навязывать укрепление хорошей репутации между собой и исключать злоумышленников. Таким образом сеть XYO снижает риски атак типа «Assassination».

---

5 Атака «Deception»

5.1 Резюме

Атака «Deception» происходит тогда, когда злоумышленник пытается передать неверные, но действительные данные, которые будут использоваться в системе для личной выгоды.

Одна из форм атаки «Deception» происходит при помощи «Multi-Chain Forging», то есть когда злоумышленник поддерживает несколько версий своей собственной цепочки, которые могут существовать в нескольких местах одновременно.

5.2 Мотивация

Злоумышленник может фальсифицировать информацию, ответвляя свою собственную геолокационную цепочку. Это может быть достигнуто путем отправки секретного ключа для одного звена цепочки, который генерируется во время создания новых локальных блоков, одному или нескольким сговорившимся противников в разных областях. Это позволяет непрерывно создавать новые геолокационные цепочки, которые исходят из одной и той же точки происхождения.

Злоумышленник может извлечь выгоду из распространения ложной информации о своем местоположении в ситуациях, когда точность местоположения является обязательной. Возьмем, к примеру, намерение построить алиби для того, чтобы подтвердить, что злоумышленник был в определенном месте в определенное время. Имея несколько цепочек, злоумышленник сможет выборочно сообщать только ту цепочку, которая несет наиболее выгодную информацию для его алиби.

5.3 Технический анализ

Атаку «Deception» становится все труднее выполнять, так как цепочка растет и становится дольше. По прошествии времени информация из определенного узла транслируется по сети XYO. Это означает, что любая возможная атака позволила бы, в лучшем случае, провести несколько небольших изменений в цепочке в заданной точке в прошлом.

Этот процесс не полностью уменьшает вероятность атаки. Во время синхронизации с мостом страж-злоумышленник может выбрать одну из своих ответвленных цепочек, которой он поделится с мостом. Поскольку обе цепочки являются действительными, мост и другие вышестоящие устройства не могут сразу же прийти к заключению, что цепочка получила ответвление. Вместо этого важно, чтобы узлы перекрестно проверяли записи сообщения с другими стражами в сети, чтобы убедиться, что узел не существовал сразу в нескольких местах.

5.4 Меры протокола по снижению рисков

Сеть XYO по своей природе может обнаруживать атаки «Multi-Chain». Любое долгосрочное ответвление цепочки узла будет несовместимым с общим консенсусом сети. Во избежание небольших изменений, когда целостность данных о местоположении имеет первостепенное значение, пользователь может дождаться дополнительных подтверждений от архивариуса, содержащих подписи из распределенных узлов. По прошествии времени все расхождения, возникающие из ответвленной цепи, станут очевидными.

5.5 Меры сети XYO по снижению рисков

Данные распространяются по всем архивариусам, которые содержат подписанные реестры сообщения между стражами. На практике обнаруживаются даже незначительные (хотя и действительные) модификации существующей цепочки. Если страж пытается выполнить атаку типа «Multi-Chain», другие узлы с противоречащими историями могут транслировать противоречие в сеть. В результате репутация стража-мошенника упадет, и все его цепочки удалятся из сети.

Таким образом, сеть XYO предназначена для обеспечения перекрестной проверки этих сообщений как меры предосторожности от этих типов атак.

5.6 Заключение

Избыточность данных в сети XYO исключает попытки транслировать противоречащие данные, уменьшая репутацию любого стража-злоумышленника до такого уровня, при котором он больше не рассматривается в сети.

---

6 Same-Machine Sybil Attack

6.1 Резюме

Атака Сивиллы с одной машины происходит тогда, когда злоумышленник создает несколько узлов из одной машины. Поскольку устройствам сети XYO не присваиваются уникальные идентификаторы, это легко достижимо. Злоумышленник усиливает репутацию, подписывая пакеты между имитируемыми узлами, чтобы показать узлы органичными и чистыми. Затем злоумышленник позволяет узлам взаимодействовать с различными группами соседних узлов таким образом, что каждый имитируемый узел хранит различную информацию в своих цепочках доказательства происхождения. Это приводит к тому, что все сымитированные узлы получают высокие оценки цепочек происхождения. Эта атака позволяет злоумышленникам недорого и массово создавать узлы, которые могут использоваться для атаки Сивиллы в локальной или даже глобальной сети.

6.2 Мотивация

Злоумышленник может предпринять атаку Сивиллы с одной машины для того, чтобы увеличить влияние на определенный регион. Создавая несколько поддельных узлов с одного и того же устройства, снижается барьер для выполнения атаки Сивиллы. Злоумышленнику гораздо проще создавать много поддельных устройств на одной машине, чем создавать множество вредоносных устройств.

6.3 Технический анализ

Нетрудно подделать информацию о Bluetooth-устройстве, чтобы сделать его неотличимой от устройства [4]. Таким образом, злоумышленник может создать несколько устройств с одного компьютера, которые действуют и выглядят как отдельные устройства.

После создания нескольких виртуальных стражей, злоумышленник может управлять стражами, как если бы они были физически различны. Стражи кажутся органичными и продолжают подписывать информацию, связанную с другими стражами

поблизости. Кроме того, злоумышленник может создать виртуальную карту устройств, которые отражаются в подписях виртуальных стражей.

6.4 Меры протокола по снижению рисков

Ключом к защите от атак Сивиллы с одной машины является способность обнаруживать повторяющиеся данные, анализируя мощность сигнала. Будет казаться, что у компьютера, на котором запущено множество виртуальных стражей, один и тот же RSSI для каждого стража. В результате, каждый виртуальный страж, работающий на компьютере, будет виден внешнему стражу, как находящийся близко друг к другу (при условии определенного колебания мощности сигнала). Чтобы предотвратить такой тип атаки, важно, чтобы легитимный страж обнаруживал связанные устройства и обрабатывал их информацию как единый узел.

6.5 Меры сети XYO по снижению рисков

Основной индикатор сети XYO для обнаружения атак Сивиллы с одной машины – это мощность Bluetooth-сигнала (RSSI). Это двухсторонняя метрика, которая может быть согласована двумя узлами. В результате узел, на котором запущена атака Сивиллы с одной машины, будет иметь одинаковую мощность сигнала для каждого из своих виртуальных узлов. Дедупликация данных узлов отсекается архивариусами, в результате чего все виртуальные узлы рассматриваются как один узел. Это делает атаку Сивиллы с одной машины неэффективной в представлении одной машины в качестве нескольких виртуальных узлов.

6.6 Заключение

Обнаружение мощности Bluetooth-сигнала сетью XYO в сочетании с возможностью дедупликации данных снижает риски атаки с машины, которая создает кластер виртуальных узлов, рассматривая кластер как единый узел.

---

7 Атака «Force Field»

7.1 Резюме

Атака «Force Field» объединяет атаку «Assassination» и традиционную атаку Сивиллы для того, чтобы посылать ложные данные в сеть. Это двойная атака: злоумышленник передает противоречащую информацию легитимным узлам, одновременно позволяя сети узлов злоумышленника выступать в качестве согласованной сети для внешних наблюдателей.

7.2 Мотивация

Этот подход принимает форму локальной атаки Сивиллы, где злоумышленник стремится полностью контролировать полномочия определенного физического местоположения. Тем не менее, чистая атака Сивиллы на сеть XYO потребует большого количества распределенных устройств с обширной историей, чтобы превзойти число существующих авторитетных узлов. Чтобы обойти это препятствие, в атаке типа «Force Field» используется гибридный подход, который сначала нацеливается на репутацию существующих узлов посредством атак «Assassination», чтобы создать противоречия между легитимными узлами.

Рассмотрим ситуацию, в которой злоумышленник хочет получить полные полномочия в определенном локальном регионе. Используя атаку типа «Force Field», злоумышленник может сначала переполнить каждый легитимный узел противоречивой информацией. Репутация этих узлов в сети будет падать, снижая квалификационный барьер репутации. Благодаря этому сниженному барьеру, злоумышленник сможет предоставить свою собственную сеть устройств, превосходящих пониженную репутацию легитимных устройств, установив единые полномочия над целевым регионом.

7.3 Технический анализ

Для того, чтобы сделать существующую сеть противоречивой, злоумышленник использует выборочное подписывание для того, чтобы уменьшить перекрытие между легитимными узлами. Этого можно достичь путем ввода вредоносных узлов в локальную сеть, а затем разрешая каждому узлу общаться только с определенными устройствами в сети. Каждый выбранный легитимный страж будет транслировать местоположение вредоносного узла, с которым он общается, в то время как вредоносный узел останется невидимым для окружающих стражей. В больших масштабах это приведет к тому, что каждый страж будет иметь совершенно иную интерпретацию состояния сети. Для такого внешнего источника, как мост, репутация каждого узла будет снижена.

Как только это будет достигнуто, злоумышленник сможет воспользоваться сниженной репутацией всей системы для того, чтобы внедрить свою собственную сеть стражей. Возможно, что эти устройства уже существовали в сети, они просто станут более значительными, когда репутация других стражей будет снижена.

Этот способ атаки зависит от количества существующих узлов в регионе и становится все более сложным по мере роста этого числа.

7.4 Меры протокола по снижению рисков

Подобно предотвращению атак «Assassination», снижение риска атак «Force Field» зависит от наказания избирательного подписывания. В атаках «Force Field» картелем вредоносных узлов используется выборочное подписывание с тем, чтобы сделать целевые легитимные узлы противоречащими сети XYO.

Когда авторитетные стражи опрашивают менее авторитетные узлы на подписи, а узлы отчетности отказываются отвечать, это уменьшает способность узлов участвовать в избирательном подписании.

Это делает выполнение атаки «Force Field» намного сложнее выполнимыми, потому что любая репутация, построенная для выполнения атаки, быстро рассеется после участия в избирательном подписывани.

7.5 Меры сети XYO по снижению рисков

Сеть XYO наказывает узлы, которые предпринимают выборочное подписывание за то, что они не соответствуют остальной системе. Это повышает стимул для узлов реагировать на запросы на подпись и вносить данные в сеть XYO. Несовместимые узлы теряют доверие в форме пониженной репутации, в результате чего компонент «Assassination» в атаке «Force Field» становится экономически невозможен. Это упрощает атаку «Force Field» до традиционной атаки Сивиллы, которая требует чрезмерного количества устройств и вычислительной мощности.

7.6 Заключение

Конечная цена для репутации стража в атаке «Force Field» в сети XYO делает атаку экономически непрактичной.

---

8 Teleportation Attack

8.1 Резюме

Атака типа «Teleportation» происходит тогда, когда злоумышленник фальсифицирует свое местоположение путем «телепортации» в другое место через сеть. Если смартфон или Bluetooth-маячок используется как страж, который предоставляет данные о местоположении злоумышленника, злоумышленник может фальсифицировать свое местоположение, отправив своего стража с кем-то другим. Если бы сеть использовалась для создания алиби, злоумышленник мог бы обменятся стражами с кем-то еще, чтобы сфальсифицировать свое переданное местоположение.

8.2 Мотивация

Этот тип атаки также может быть проведен на уровне программного обеспечения, когда злоумышленник поделится своим секретным ключом с одним или несколькими лицами. Если бы сеть использовалась для проверки отзывов об отелях, это позволяло бы людям оставлять отзывы, у которых имеется заслуживающая доверия история в цепочке. Злоумышленник может удаленно поделиться своим секретным ключом с кем-либо в отеле, и может действовать так, как если бы он находился там, не находясь в непосредственной близости от него.

8.3 Технический анализ

Если пользователю предоставляется секретный ключ, то его можно использовать для создания поддельного устройства, которое будет отображаться так, как будто это устройство пользователя. Использование программного-управляемой радиосистемы позволит участникам, имеющим право на участие, отображаться как любое конкретное устройство в сети, при условии, что оно связано с секретным ключом этого устройства. Это аннулирует попытки проверить местоположение пользователя. Это также может повлиять на данные в блокчейне, поскольку во время атаки «Teleportation» теоретически трудно распознать легитимное перемещение устройства.

8.4 Меры протокола по снижению рисков

Стратегии обнаружения против такого типа атаки сложны из-за естественных разрывов в цепочке. Например, если телефон используется как страж, и он отключен, он не будет связываться с сетью, пока не будет включен снова. Промежутки в отправляемой информации требуют сложного алгоритма, позволяющего отличать естественные промежутки от потенциально опасных точек ввода данных, которые должны быть наказаны.

8.5 Меры сети XYO по снижению рисков

Возможность атаки «Teleportation» начинается снижаться в тот момент, когда архивариусы могут обмениваться информацией друг с другом и проверять жизнеспособность данных. Дополнительно снижается количество подходящих вышестоящих в сети устройств, где серверы могут сравнивать данные по крупным географическим регионам. Это позволяет провидцам видеть плохие данные в виде дублированных местоположений и телепортации, которые могут быть отфильтрованы и наказаны с использованием алгоритма.

8.6 Заключение

В то время, как атаку «Teleportation» трудно определить на уровне протокола, серверы более высокого уровня в сети XYO, такие как архивариус, позволяют обнаруживать и наказывать вредоносные данные в сети. Обмен информацией между этими серверами будет постоянно строить и добавлять доверенную информацию для фильтрации плохих данных из системы.

---

9 Атака «Stealth»

9.1 Резюме

Атака «Stealth» определяется устройством, маскирующимся от сети. Различные варианты применения сети XYO требуют, чтобы устройства в сети имели целостную историю цепочки.

9.2 Мотивация

У злоумышленника мало стимулов совершать атаки «Stealth» на сеть XYO. Сеть стремится обеспечить уверенность в том, что что-то существует в определенном месте, а не повсюду. Это важное различие, поскольку данные на уровне протокола могут быть неточными, потому что узлы утратили доверие.

Тем не менее, злоумышленник может стратегически включать и отключать службы определения местоположения в своем телефоне или маячке для того, чтобы создать плохую цепочку данных, которые в противном случае выглядели бы действительными. Это, по сути, позволит им спрятаться от сети, если они не хотят сообщать данные и заново появляться в сети тогда, когда это выгодно для них.

9.3 Технический анализ

Атака «Stealth» может быть достигнута путем выключения устройства в сети. Более сложным подходом может быть использование клетки Фарадея, которая скрывает устройство от сети. Нефизический подход к такому типу атаки может быть достигнут с помощью атаки «Отказ в обслуживании».

9.4 Меры протокола по снижению рисков

Действия против атаки «Stealth» могут быть сложными из-за того, что Bluetooth и другие устройства можно легко отключить от сети. Основной стратегией по устранению этой уязвимости является внедрение и использование сильного программного слоя, который наказывает стражей и мосты, которые передают данные о неработающих цепях. Средства обнаружения будут учиться и расти со временем, поскольку алгоритм станет лучше понимать тонкие различия между действительными и недействительными данными.

9.5 Меры сети XYO по снижению рисков

Промежуток в истории узла будет явно подозрительным в тех случаях применения, которые требуют непрерывного подтверждения местоположения в сети XYO. Когда данные доходят до архивариусов, они подвергаются строгому процессу отсеивания и фильтрации, который может выявлять эти промежутки и наказывать за несоответствия. Эта основная особенность сети XYO позволяет обеспечить наиболее точное местоположение, несмотря на беспорядочные данные, присущие физическому миру.

9.6 Заключение

Учитывая случаи применения сети XYO, атака типа «Stealth» экономически не оправдана.

10 Атака «Отказ в обслуживании»

10.1 Резюме

Атака «Отказ в обслуживании» (DoS) происходит тогда, когда вредоносный или плохо функционирующий субъект вызывает локальный, региональный или системный отказ.

10.2 Мотивация

Злоумышленник может попытаться нарушить работу сети XYO, чтобы лишить ее возможности проверить доказательство местоположения.

10.3 Технический анализ

Из-за характера протокола Bluetooth, Bluetooth-маячки могут одновременно подключаться только к одному устройству. Это означает, что любое устройство, которое принимает неаутентифицированные команды, может быть легко отключено от сети. Это может быть достигнуто за счет использования приложения для мобильных телефонов, которое позволит одному устройству, которое передает Bluetooth-команды, делать это постоянно с относительной легкостью. Отправка шестнадцатеричных значений устройству для заданных параметров, таких как параметр «воспроизведение звука» на большинстве маячков, создает соединение с этим устройством. Если это соединение установлено, оно блокирует связь любого другого устройства с ним. Это можно усилить с помощью программного-управляемой радиосистемы, которая могла бы запускать скрипты для непрерывной трансляции различных шестнадцатеричных значений на любой сетевой маячок в диапазоне.

10.4 Меры протокола по снижению рисков

Bluetooth-устройства в сети XYO должны принимать только аутентифицированные команды или использовать белый список MAC-адресов. Уменьшение количества команд, не прошедших проверку подлинности, сводит к минимуму доступ к этому вектору атаки.

10.5 Меры сети XYO по снижению рисков

Сеть XYO состоит из пользователей, которые запускают серверы архивариусов и провидцев. Оба этих компонента делятся информацией и проверкой со своими узлами. Это позволяет создать запрос на выбор из любого «стека» компонентов для получения ответа. Несмотря на то, что можно отклонять небольшую часть сетевой службы на уровне протокола, ширина и масштаб сети делают это экономически нецелесообразным.

10.6 Заключение

Из-за распределенного характера сети XYO, сеть остается работоспособной несмотря на попытку совершить атаку «Отказ в обслуживании». Поскольку DoS требует высокой вычислительной мощности и физического доступа для атаки на целый стек, нацеливание

даже на небольшую часть сети XYO является дорогостоящим и экономически нелогичным.

---

11 Благодарность

Данный Красный документ является дополнением по безопасности Проектного документа сети XYO и Зеленого документа сети XYO. Мы благодарим Кристин Сако за внимание к деталям и применение передового опыта в ее обзоре данной работы.

Справочная литература

[1] Джафрания-Джароми, Али. Али Брумандан, Джон Нильсен и Жерар Лашапель. Уязвимость GPS к угрозам спуфинга и обзор анти-спуфинговых методик. https://www.hindawi.com/journals/ijno/2012/127072/cta/ Международный журнал навигации и наблюдения, Альберта, Канада, май 2012 года.

[2] Паджетт, Джон, Джон Бар, Майанк Батра, Марсель Холтманн, Ронда Смитбей, Лили Чен и Карен Скарфоне. Справочник по безопасности Bluetooth. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf U.S. Департамент коммерции, Наицональный институт стандартов и технологии, май 2017 года.

[3] Даннинг, ДжП. Взламывая Bluetooth от скуки. https://www.defcon.org/images/defcon-18/dc-18-presentations-/Dunning/DEFCON-18-Dunning-Breaking-Bluetooth.pdf DefCon, август 2010 года.

[4] haxf4rall. Спуфинг Bluetooth-устройства. http://haxf4rall.com/2016/05/11/spoofing-a-bluetooth-device/ 11 мая 2016 г.

[5] Начальник органа принудительного исполнения. Советник принудительного исполнения FCC. https://apps.fcc.gov/edocs public/attachmatch/DA-14-1785A1.pdf FCC.gov, 8 декабря 2014 года.

Словарь

Точность
Мера уверенности в том, что точка данных или эвристики находится в пределах определенной погрешности.

Архивариус
Архивариус сохраняет эвристику как часть децентрализованных данных с целью хранения всей истории реестров, но без этого требования. Даже если некоторые данные теряются или становятся временно недоступными, система продолжает функционировать, только с пониженной точностью. Архивариусы также индексируют реестры, чтобы они при необходимости могли возвращать строку данных реестра. Архивариусы хранят только исходные данные и получают оплату исключительно за получение данных. Хранение всегда бесплатное.

Мост
Мост - это транскриптор эвристики. Он безопасно передает эвристические реестры от стражей до провидцев. Важнейшим аспектом моста является то, что провидец может быть уверен в том, что эвристические реестры, полученные от моста, никоим образом не были изменены. Второй важнейший аспект моста - это прикрепление дополнительных метаданных доказательства происхождения.

Достоверность
Оценка вероятности того, что точка данных или эвристика не была скомпрометирована или взломана.

Криптоекономика
Формальная дисциплина, которая изучает протоколы, которые управляют производством, распределением и потреблением товаров и услуг в условиях децентрализованной цифровой экономики. Криптоекономика - это практическая наука, которая фокусируется на разработке и характеристике этих протоколов.

Провидец
Провидец отвечает на заданный запрос, анализируя предварительные данные, хранящиеся в сети XYO. Эвристика, хранящаяся в сети XYO, должна иметь высокий уровень доказательства происхождения для определения достоверности и точности эвристики. Провидец получает и предоставляет ответ, исходя из оценки свидетеля на основании его доказательства происхождения. Учитывая, что сеть XYO не требует доверия, провидцы должны быть заинтересованы в обеспечении честного анализа эвристики. В отличие от стражей и мостов, для добавления ответов в блокчейн провидцы используют доказательство выполненной работы.

Оценка цепочки происхождения
Оценка, которая присваивается цепочке происхождения для определения его подлинности. Эта оценка учитывает длину, переплетение, перекрытие и избыточность.

Цепочка доказательства происхождения
Цепочку переходного ключа, которая связывает вместе серию связанных свидетелей эвристических записей реестра.

Страж
Страж - это эвристический свидетель. Он наблюдает за эвристикой и отвечает за достоверность и точность, создавая временные реестры. Важнейший аспект стража заключается в том, что он создает реестры, в которых провидцы могут быть уверены в том, что они происходят из одного и того же источника, добавляя к ним доказательство происхождения.

Не нуждающийся в доверии
Такая характеристика, когда все стороны в системе могут достичь консенсуса относительно того, что является канонической истиной. Власть и доверие распределяются (или распространяются) среди заинтересованных сторон сети (например, разработчики, майнеры и потребители), а не концентрируются в одном физическом или юридическом лице (например, в банках, правительствах и финансовых учреждениях). Это общий термин, который легко можно неправильно понять. Блокчейны не самом деле не устраняют доверие. Их работа заключается в минимизации количества доверия, требуемого от любого отдельного участника системы. Это достигается путем распространения доверия среди различных участников системы через экономическую игру, которая стимулирует субъектов сотрудничать по правилам, определяемым протоколом.

Сеть XYO
Сеть XYO расшифровывается, как «Сеть оракулов XY». Она включает всю систему компонентов/узлов XYO, в состав которых входят стражи, мосты, архивариусы и провидцы. Основная функция сети XYO - быть порталом, с помощью которого цифровые смарт-контракты могут выполняться через подтверждение географического расположения в реальном мире.