 **МИНОБРНАУКИ РОССИИ**

**федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Самарский государственный технический университет»**

**(ФГБОУ ВО «СамГТУ»)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

TheOoL.net

*Оракул Свободы –безопасная распределенная операционная система*

Руководитель проекта:

Алексей Ненашев

Презентующий:

Студент 3-ТЭФ-1

Темников Егор Алексеевич

Самара, 2019 г.

Не секрет, что IP-сети создавались как открытые и децентрализованные с полным отсутствием политики безопасности. При этом сетевой протокол позволяет злоумышленнику анализировать топологию сети, определить какие операционные системы и приложения исполняются на конкретных узлах сети, собрать сведения об их аппаратном обеспечении. Сбор такого рода информации позволяет локализовать узлы потенциально интересные для атаки по принадлежности целевой жертве и наличию возможных уязвимостей.

В противоположность сетям большинство современных систем хранения и обработки данных повторяют архитектуру корпораций-пользователей и построены в централизованной архитектуре или имеют центры управления. Для закрытия противоречия между архитектурой IP сети и потребностями современных информационных систем и удобства работы пользователей разработано множество дополнительных служб и сервисов, предназначенных для централизации управления сетью и программной инфраструктурой, построения приватных сетей и т.п., каждый из которых аккумулирует сведения о работе узлов и пользователей сети и использует их для облегчения работы ИС и управления сетью. И сверху все прикрыто плотным слоем узкоспециализированных подсистем кибербезопасности, нацеленных на закрытие той или иной уязвимости, либо класса уязвимостей, что влечет за собой: проблемы интеграции защитных подсистем с программным обеспечением и друг другом и служит источником уязвимостей безопасности информации за счет ошибок при настройке системы безопасности.

Очевидно, что в этой ситуации обладание сведениями о принадлежности узлов и их программном и аппаратном обеспечении существенно облегчает задачу потенциального злоумышленника.

Несмотря на известные проблемы безопасности Интернет продолжается внедрение сервисов интернета вещей и интернета всего. Повсеместно внедряются автоматические системы для управления объектами повышенной опасности, такие как беспилотный транспорт, промышленные роботы, и системы «умного дома», оснащенные камерами и автоматикой для управления электроснабжением, отоплением и физическим доступом в помещения, в том числе в массовом бюджетном жилье. Что в свою очередь расширяет спектр возможных угроз вплоть до угрозы физической безопасности людей и объектов бытовой и промышленной инфраструктуры.

Современные системы хранения и обработки данных построены, в основном, в централизованной архитектуре , либо имеют центры управления, контроль над которыми может быть перехвачен через аппаратные, либо программные уязвимости или внедрением в состав технического персонала агентов

Если брать примеры из теплоэнергетики, то по количеству сигналов на станции можно вычислить компьютер оператора и главный, что в свою очередь дает доступ ко всей информации на объекте или же к управлению самим объектом(ТЭЦ) и информацией на объекте. Все это создает опасную аварийную ситуацию, ведь если выйдут из строя важные датчики или с них не будет приходить сигнал на пульт управления (сигнал может быть искажен). Это особенно важно из-за повсеместного внедрения цифровых систем управления.

В связи с этим и ведется разработка нашего проекта .

Одноранговая распределенная система хранения и обработки защищаемой информации (ОРСХОЗИ) или же TheOoL.net.

Одноранговая распределенная система хранения и обработки защищаемой информации (ОРСХОЗИ) предназначена в первую очередь для устранения угроз информационной безопасности (ИБ) нацеленных на серверы , центральные вычислительные узлы и абонентские места сети со стороны двух классов злоумышленников: 1. Внешние нарушители ИБ; 2. Внутренние нарушители ИБ, которых можно разделить на 2 подкласса: технический персонал вычислительных узлов и прочие сотрудники. Предлагаемое техническое решение представляет собой распределенную операционную систему, каждый узел которой отдает свои вычислительные ресурсы (подсистему хранения, центральный и графический процессоры, оперативную память) системе и не имеет самостоятельного значения. Однако различие между узлами присутствует по двум параметрам:

1. Функциональному назначению. Может быть узлом абонента (одновременно выполняет и функции узла хранения), узлом хранения и узлом метаданных. Определяется на этапе имплементации узла системы.

2. По рангу. Ранг вычисляется относительно каждого узла абонента динамически в зависимости от требуемого клиентской задачей параметра производительности и скорости доступа по сети.

TheOoL осуществляет качественный переход от информационной компьютерной сети (Internet) к единой информационной экосистеме, построенной на принципах:

1. Первичности пользовательской информации: алгоритмы взаимодействия пользователя с сетью должны реализовывают непосредственную работу с пользовательской информацией через упорядоченную информационную картотеку без взаимодействия с узлами сети, либо ее техническими службами. Сама процедура работы с информационной картотекой максимально унифицирована и стандартизирована.

2. Живучести пользовательской информации: информация не может быть потеряна или уничтожена никаким способом кроме прямой команды на уничтожение информации от пользователя, который ее опубликовал, либо лица специально им уполномоченного.

3. Доступности пользовательской информации: весь доступный пользователю контент автоматически попадает в информационную картотеку пользователя. Для каждого пользователя формируется индивидуальная информационная картотека.

4. Защищенности пользовательской информации: пользователь сам решает какую персональную информацию и какой, созданный им, контент сети будет раскрыт другим пользователям. Он же определяет и взаимосвязи между опубликованными им данными. Изначально вся информация считается закрытой и доступной только самому пользователю – владельцу. Фактически принцип предполагает так же возможность анонимной публикации контента и сокрытие фактов чтения контента. Тут следует отметить, что сведения об общей статистике чтения контента и оценках

контента, не раскрывая при этом читателей и оценщиков, должны предоставляться владельцу контента для оценки релевантности информации для ее целевой аудитории.

5. Хранения пользовательской информации «везде и нигде»: принцип следует из необходимости обеспечения живучести и защищенности пользовательской информации и предполагает распределенное хранение и обработку информации в сети, организованные таким образом, чтобы ни одно устройство сети не обладало ни одной конечной единицей контента полностью. Любой документ в сети должен быть разделен на части достаточно малые, чтобы обеспечить невозможность восстановления целого по его части. И затем эти части должны быть распределены между узлами сети так, чтобы ни один узел не владел больше чем одной такой частью.

6. Полной абстракции пользователей от метаданных, технической информации, процессов функционирования сети: принцип предполагает полную, с точки зрения пользователя, независимость пользовательской информации от ее физических и логических носителей. Иначе говоря, пользователь должен получать непосредственный доступ к полезному контенту минуя обращение к какому-либо узлу или адресу сети через единую упорядоченную информационную картотеку.

7. Полного сокрытия от пользователей метаданных и технической информации: принцип предполагает блокировку любых возможностей анализа топологии и структуры сети и полное сокрытие технической информации о работе сети и ее программного обеспечения в том числе и от технических специалистов. Исполнение этого принципа предполагает автоматическое выполнение всех сервисных мероприятий сети и программ. Единственным исключением должны быть сведения о состоянии аппаратного обеспечения узлов, которые должны транслироваться в каталог пользователя – владельца. Это необходимо, чтобы обеспечить функциональную возможность контроля за техническим состоянием устройств и обеспечением их своевременного ремонта или замены. Вторая функция такого исключения - контроль общей нагрузки на аппаратных мощностях для их своевременного увеличения. Сокрытие метаданных означает отсутствие у кого-либо из пользователей любой информации о точных местах хранения частей документов.

В представленной обобщенной архитектуре единой информационной экосистемы за реализацию принципов 1 – 5 отвечает «Протокол распределенной обработки информации», который также отвечает за сокрытие от пользователей метаданных системы хранения и обработки. За реализацию принципов 6,7 отвечает «защищенный сетевой протокол».

С точки зрения реализации сетевого протокола система представляет собой одноранговую сеть с переменной длинной адреса и динамической переменной адресацией, в которой узлы не имеют самостоятельного значения, а отдают свои вычислительные ресурсы облаку вычислений и хранения TheOoL. Узлы сети не имеют никаких демаскирующих признаков. Обработка метаданных сети происходит на уровне протокола распределенной обработки информации с применением шифрования и маскировки в рамках кластеров метаданных, которые, в свою очередь периодически «переезжают» по сети. Узел периодически в автоматическом режиме принимает роли узла хранения данных или узла метаданных.

Пользователи работают в изолированной от сети операционной системе под управлением виртуальной машины, все ресурсы сети для которой представляются локальными. Это позволяет полностью заблокировать доступ со стороны злоумышленников к уязвимостям пользовательского ПО и блокирует сетевые руткиты.

Для обеспечения обратной совместимости с существующим ПО TheOoL предоставляет 3 интерфейса доступа к информации: иерархический (для имитации файловой системы), SQL (для имитации доступа к данным в реляционной модели, в которой реализовано большинство современных бизнес-приложений) и NoSQL (для имитации документо-ориентированной модели хранения данных, используемой в системах BigData). При этом, с точки зрения пользовательской ОС, СУБД представляется локальной, а распределенная файловая система – локальным диском.

Для обеспечения дополнительной защиты ОРСХОЗИ блокирует стандартные сетевые протоколы. Работа пользователя ОРСХОЗИ происходит под управлением пользовательской операционной системы (ПОС). В качестве ПОС допускается любая операционная система, используемая на предприятии. ПОС исполняется под управлением виртуальной машины (ВМ) из состава программного обеспечения узла ОРСХОЗИ и полностью изолируется от сети. А любые ресурсы, включая сетевые устройства ввода-вывода, систему хранения и интерфейс РРСУБД, передаются ПОС как локальные. Таким образом: блокируются уязвимости программного обеспечения, исполняемого под управлением ПОС, и функционал вредоносного ПО нацеленный на хищение данных пользователя с их последующей скрытой передачей удаленному получателю; маскируется топология сети предприятия от пользователя и внешнего нарушителя; ИС предприятия не требуют замены и существенной доработки. Взаимодействие с внешними сетями допустимо через специальные шлюзы, выполняющие функции маршрутизации и межсетевого экранирования (МЭ) на канальном уровне модели передачи ISO/OSI.

Хранение данных в ОРСХОЗИ осуществляется таким образом, что любой файл разделяется на N блоков, шифруется и отправляется на хранение на K\*N узлов сети (K - коэффициент избыточности). При этом шифрованию подвергаются в том числе и данные в оперативной памяти, за исключением минимального оперативного блока. Перечень узлов хранения блоков помещается в блок метаданных, который в свою очередь шифруется и помещается на узлы метаданных. Блоки периодически, в периоды пониженной нагрузки сети в автоматическом режиме перемещаются между узлами. Таким образом никто, включая владельца, не знает, на каких узлах в конкретный момент времени хранятся части файла, кроме подсистемы, имеющей доступ к метаданным. Для обеспечения дополнительной защищенности этой информации, ключи шифрования метаданных меняются динамически с установленной периодичностью. Таким образом собрать полный файл становится задачей почти невыполнимой, но в случае, если такое событие все же произойдет, файл будет зашифрован сильным алгоритмом шифрования. С учетом автоматической генерации ключей шифрования и их повышенной длине (не ниже чем 1024 бит), дешифровка файла является крайне сложной задачей, а положительный результат маловероятным.

В случае выхода из строя любого узла, для блоков, которые хранились на нем, определяются новые места хранения, и они автоматически копируются туда с избыточных узлов. То есть потеря блока возможна только при одновременном выходе из строя всех K узлов, где он хранится. При этом к данным относятся не только пользовательские данные, но и программное обеспечение. Таким образом технический отказ узла будет означать всего лишь быструю установку программного узла на новое железо и имплементацию (регистрацию) узла в ОРСХОЗИ, после чего пользователь будет иметь доступ ко всем своим программам, настройкам и данным автоматически.

Таким образом, за счет шифрования, динамической маскировки данных, динамической избыточности, распределенности хранения и одноранговости, с точки зрения пользователя и нарушителя, узлов ОРСХОЗИ, а так же за счет встроенных в систему алгоритмов предотвращения несанкционированного доступа к узлам и данным и подсистемы защищенного и анонимного (с технической точки зрения) доступа к ресурсам вне ОРСХОЗИ, разрабатываемая система будет устойчива ко всем известным типам атак и методов несанкционированного съема информации по техническим каналам утечки с узлов ОРСХОЗИ. А при должной организации технической защиты информации на абонентских узлах от съема информации до момента применения алгоритмов шифрования к данным и должных организационных мер направленных на защиту информации, будет обеспечена полная защищенность сведений. И при высоком уровне защищенности данных ОРСХОЗИ обеспечит достаточно высокое быстродействие для комфортной работы алгоритма за счет подсистемы оптимального управления производительностью на уникальном алгоритме динамической оптимизации производительности.

Все это значит, что в TheOol.net отсутствую места, где храниться полная информация (файл, документ), а вся информация «размазана и перемешана» по всей системе и собирается в документ только при помощи «ключа», что дает доступ к данным только владельцу ключа. В то же время владелец имеет право указать количество информации и доступ к ней, сделать общедоступной или же только для отдельных пользователей с помощью дочерних ключей.

В проекте TheOol.net я совместно с Ростиславом Олешко занимаемся разработкой протокола сетевого уровня, заменяющего IP-протокол на базе операционной системы UBUNTU 18-04 и его ядра Linux 5.3.8.