**Лекция 12**

**Анализ сетевой безопасности**

*Приведены результаты анализа сетевой безопасности эталонной архитектуры туманных вычислений. Рассматриваемая архитектура представлена консорциумом OpenFog, в который входят такие ведущие компании, как Intel, Dell, Microsoft, Cisco и др. В архитектуре описаны типы связи Node-to-Node, Node-to- Cloud. В ходе анализа архитектуры были исследованы вопросы безопасности следующих типов связей: Node-to-Node, Node-to-Cloud и Node-to-Device. Для каждого типа связи были рассмотрены протоколы без- опасности и выявлены возможные угрозы и уязвимости. Также приведены выводы о потенциальных ме- тодах защиты. Кроме того, в работе была рассмотрена предполагаемая модель угроз OpenFog Reference Architecture, описывающая типы угроз, уровни их реализации и аспекты безопасности.*

**Безопасность туманных вычислений, атаки на туманные вычисления, архитектура туманных вычислений, архитектура OpenFog RA, анализ сетевой безопасности туманных вычислений, связи в туманных вычислениях**

Развитие концепции Internet of Things (IoT) послужило толчком для распространения различ- ных типов устройств в компьютерных сетях по всему миру. Как правило, подобные устройства генерируют большое количество неоднородных, зашумленных данных. Информация, поступаю- щая с подобных устройств, обычно обрабатыва- ется центрами обработки данных (ЦОД), часто с использованием облачных технологий. Однако в последнее время получила развитие концепция так называемых туманных вычислений.

Туманные вычисления – это горизонтальная ар- хитектура системного уровня, которая распределяет ресурсы и службы (такие как вычисления, хранение данных, управление и организация сети) между облачной вычислительной средой (ОВС) и конеч- ным устройством/узлом. Данная архитектура осно- вана на моделях IoT, 5G и ориентирована на задачи, требованиями к которым являются:

* ограниченные вычислительные ресурсы;
* высокая пропускная способность сети;
* сверхнизкая задержка прохождения сигнала;
* повышенные меры безопасности.

Этот подход расширяет традиционную модель облачных вычислений, позволяя выполнять обра- ботку данных локально. Туманные вычисления сохраняют все преимущества облачных вычисле- ний, таких как контейнеризация, виртуализация, оркестровка, управляемость и эффективность [1]. Туманная модель вычислений перемещает обра- ботку данных и принятие решений из облака ближе к оконечным узлам, вплоть до датчиков и исполнительных механизмов IoT.

В данной статье описывается архитектура ту- манных вычислений, рассматриваются типы связей и проводится анализ их сетевой безопасности. Кро- ме того, предлагается интеграция инфраструктуры открытых ключей в туманные вычисления.

**Эталонная архитектура OpenFog.** На сего- дняшний день разработкой концепции туманных вычислений занимаются множество ведущих IT- компаний, такие как Cisco Systems, Intel, Microsoft Corporation, Dell и др. В 2015 г. компаниями был создан консорциум OpenFog. Одна из главных задач этой организации – разработка системной архитектуры для туманных вычислений и прора-

ботка методов практического внедрения новой модели вычислений. В результате работы консор- циум представил эталонную архитектуру туман- ных вычислений OpenFog Reference Aechitecture (OpenFog RA).

Эталонная архитектура OpenFog RA – это ар- хитектура, затрагивающая средний и высокий уровень абстракции и разработанная для туман- ных узлов и сетей. Данная архитектура представ- лена на рис. 1.



Global (Internet/Cloud/Servers)

Core Network Core Network

* Node-to-Cloud;
* Node-to-Node;
* Node-to-Device.

*Соединение Node-to-Cloud* сохраняет протоколы интернет-коммуникаций и API-интерфейсы, кото- рые используются облачными серверами для взаи- модействия с внешними устройствами (включая устройства IoT, персональные мобильные устрой- ства, терминалы, автономные компьютеры и серве- ры). Почти все эти коммуникации в настоящее вре- мя осуществляются с помощью наборов протоко- лов, представленных в табл. 1.

*Таблица 1*

|  |  |  |
| --- | --- | --- |
| Приложения | Протокол | |
| передачи  данных | безопасности |
| Для предприятий | SOAP over  HTTP | WSS |
| Мобильные  и пользовательские | RESTful  HTTP/COAP | TLS/DTLS |

Edge Nodes

Edge Nodes

*Рис. 1*

Edge Nodes

Как видно из табл. 1, протоколы относятся к прикладному уровню.

*Соединение Node-to-Node*. Распределенная ту-

OpenFog RA устанавливает набор основопо- лагающих принципов, которые называются Pillars (столпы/колонны):

* + безопасность;
  + масштабируемость;
  + открытость;
  + автономия;
  + RAS (надежность, доступность, удобство обслуживания);
  + гибкость;
  + иерархичность;
  + программируемость.

Эталонная архитектура OpenFog RA пред- ставляет собой совокупность туманных узлов, включающих гибкую систему соединений и фи- зически не привязанных к сети.

Архитектура туманных вычислений находит широкое применение в различных отраслях и рынках (среди них транспорт, сельское хозяйство, смарт-города, интеллектуальные здания, здраво- охранение, гостиничный бизнес, энергетика и финансовые услуги). Она обеспечивает реализа- цию бизнес-проектов для приложений IoT, кото- рые требуют принятий решений в реальном вре- мени, низкую задержку, повышенную безопас- ность и ограниченный трафик сети.

Рассмотрим различные типы связей между узлами в туманных вычислениях. Можно выде- лить три типа связей [1]:

манная вычислительная платформа (ТВП) может состоять из иерархии туманных узлов, охватываю- щих несколько интернет-подсетей или администра- тивных доменов. Эти узлы ТВП должны взаимо- действовать друг с другом, используя шаблон изда- тель-подписчик (на основе событий) и клиент- серверных сообщений, что позволит обеспечить прямое и своевременное взаимодействие. Для реа- лизации этих парадигм обычно используются стеки протоколов, представленные в табл. 2.

*Таблица 2*

|  |  |  |
| --- | --- | --- |
| Приложения | Протокол | |
| передачи данных | безопасности |
| Клиент-сервер | SOAP, RESTful  HTTP/COAP | WSS, TLS/DTLS |
| Издатель-  подписчик | MQTT, AMQP, RTPS | TLS/DTLS |

Исходя из представленных данных, можно сделать вывод о том, что безопасность связи бу- дет базироваться на безопасности протоколов TLS/DTLS и WSS.

*Соединение Nod-to-Device*. Данная связь описы- вает соединение между узлом и конечными устрой- ствами. Эти устройства могут быть связаны с узлом с помощью различных коммуникационных прото- колов (через различные коммуникационные среды). С использованием стека протоколов (TCP/UDP/IP) были предприняты усилия по конвергенции прото- колов между беспроводными сетями, проводными сетями и промышленной автоматизацией.

Также существуют устройства, не адаптиро- ванные к интернет-протоколам со строго ограни- ченными ресурсами. Таким устройствам доступ- но только ограниченное множество криптографи- ческих функций (симметричные шифры, которые используют установленные вручную ключи). Эти устройства должны быть установлены в физиче- ски защищенных средах и подключены через ап- паратные соединения к одному или нескольким узлам тумана, которые могут обеспечить боль- шинство служб безопасности.

В табл. 3 представлены протоколы взаимо- действия для связи Node-to-Device.

*Таблица 3*

|  |  |
| --- | --- |
| Уровень | Протоколы |
| PHY & MAC Layer | WLAN: 802.11, WPAN:  802.15, PLC: PRIME,  Automation: CIP |
| Wireless Protocol Stacks | Wi-Fi, Bluetooth, ZigBee |
| Adaptation Layer | WLAN/WPAN: 6LowPAN, PLC: PRIME  IPv6 SSCS, Automation: Ethernet/IP |
| Transport/Network Layers | UDP over IPv6, TCP  over IPv6, IPv6 Stack |
| Application Layer (Publish- Subscribe Messaging) | CoAP, MQTT, AMQP, RTPS |
| Routing | RPL, PCEP, LISP  (Cisco) |
| Security | 802.1AR – Secure De- vice Identity  802.1AE – Media Access Control (MAC) Security 802.1X – Port-Based (Authenticated) Media Access Control  IPsec AH & ESP, Tun- nel/Transport Modes (D)TLS – (Datagram)  Transport Layer Security |

Из табл. 3 следует, что самым распространен- ным протоколом беспроводной связи является протокол Wi-Fi. Поэтому при анализе данного типа связи этот протокол будет рассматриваться как протокол передачи данных.

**Безопасность туманных вычислений.** Без- опасность – важнейший аспект туманных вычис- лений. Для обеспечения базовой функциональной совместимости должны существовать общие по- ложения, которые будут учитывать региональные и государственные требования по безопасности. На их основе будет базироваться безопасность туманных вычислений.

Одним из основополагающих принципов без- опасности OpenFog RA является криптография.

Для того чтобы гарантировать на базовом уровне совместимость компонентов туманных вычисле- ний, OpenFog RA адаптирует спецификацию FIPS 140-2 [2], которая содержит требования к безопас- ности для криптографических модулей. В ней опре- делен список криптографических функций, а также алгоритмы их применения. Ответственность за сер- тификацию криптографических модулей ляжет на поставщиков и изготовителей.

Криптографический модуль OpenFog должен поддерживать минимальный набор следующих функций:

* симметричное шифрование: AES (128-bit), Triple-DES;
* асимметричное шифрование: DH, RSA, DSA;
* шифрование на эллиптических кривых: ECDH, ECDSA, ECQV;
* криптографические хэш-функции: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA- 512/256;
* генератор случайных чисел;
* аутентификация сообщений: CCM, GCM, GMAC6, CMAC, HMAC.

Для защиты соединений в эталонной архитек- туре OpenFog выделен отдельный уровень – защита соединений. На данном уровне реализуются ком- муникационные службы безопасности, описанные в рекомендациях X.800 [3] для всех физиче- ских/виртуальных каналов связи среди всех объек- тов в иерархии Device-Fog-Cloud Computing:

* Конфиденциальность:
* сетевого соединения;
* сетевых пакетов;
* сетевого трафика.
* Целостность:
* сетевого соединения с восстановлением;
* сетевых пакетов (с возможностью обнару- жения).
* Аутентификация:
* сетевого пакета (подтверждение правильно- сти источника);
* сетевого соединения.
* Неотказуемость:
* источника;
* получателя.

Для реализации данных служб безопасности используются механизмы безопасности, пред- ставленные в табл. 4.

В данной таблице используется два вида обо- значений: «+» – механизм используется для реа-

*Таблица 4*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Служба безопасности | Механизм защиты | | | | | |
| Шифрование | ЭЦП | Контроль целостности данных | Дополнение трафика (padding) | Контроль маршрутизации | Нотари- зация |
| Конфиденциальность сетевого соединения | + | – | – | – | + | – |
| Конфиденциальность сетевых пакетов | + | – | – | – | + | – |
| Конфиденциальность сетевого трафика | + | – | – | + | – | – |
| Целостность сетевого соединения с восстановлением | + | – | + | – | – | – |
| Целостность сетевых пакетов | + | + | + | – | – | – |
| Аутентификация сетевого пакета | + | – | – | – | – | – |
| Аутентификация сетевого соединения | + | – | – | – | – | – |
| Неотказуемость источника | – | + | + | – | – | + |
| Неотказуемость получателя | – | + | + | – | – | + |

*Таблица 5*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Угроза | Аспект безопасности | | | |
| Конфиденциальность | Целостность | Доступность | Аутентификация |
| Инсайдеры | Утечка данных | Изменение данных | Предоставление недоступных ресурсов | Подмена данных |
| Атаки  на аппаратном уровне | Трояны, атака по сторонним каналам | Трояны | Радиопомехи, исчерпание полосы пропускания | Трояны |
| Атаки на программное обеспечение | Вредоносное программное обеспечение | Вредоносное программное обеспечение | DoS/DDoS, истощение ресурсов | Вредоносное программное обеспечение, социальная инженерия |
| Сетевые атаки | Прослушивание, анализ сетевого трафика | Пересылка сообщений | DoS/DDoS, Subnet Flooding | Spoofing, Man-in-Middle  Attacks |

лизации данной функции безопасности; «–» – механизм не предназначен для реализации дан- ной функции безопасности.

Таким образом, при реализации требований механизмов безопасности X.800 будет обеспечена конфиденциальность, целостность, аутентифика- ция и неотказуемость передачи сообщений.

**Анализ безопасности.** В эталонной архитек- туре OpenFog RA приводится предполагаемая модель угроз. Она описывает типы угроз, уровни их реализации и аспекты безопасности, к кото- рым относятся угрозы [1]. Модель угроз пред- ставлена в табл. 5.

Туманные вычисления представляют собой распределенную сеть, поэтому стоит уделить

особое внимание сетевой безопасности. В [4] и

1. отмечается уязвимость туманных вычислений к атаке «человек посередине» (Man-in-Middle At- tacks, MITM). Также в статьях заостряется вни- мание на том, что данная атака может быть про- ведена практически незаметно для потенциаль- ной жертвы. Обе статьи вышли до опубликования эталонной архитектуры туманных вычислений, и в них не учитывается то, что в Open Fog RA при- няты рекомендации X.800, которые устанавлива- ют требования к строгой аутентификации соеди- нения (сетевым пакетам), а также к шифрованию каналов связи. С учетом принятых требований и рекомендаций OpenFog RA проведение описан- ной в статьях атаки маловероятно.

Рассмотрим каждый тип связи эталонной ар- хитектуры с точки зрения сетевой безопасности.

*Node-to-Cloud* и *Node-to-Node*. В обоих типах связи используется протокол безопасности TLS/DTLS, обеспечивающий конфиденциаль- ность, аутентификацию и целостность соедине- ния. На данный момент существует три типа ата- ки на TLS/DTLS: Bar Mitzvah [6], Logjam [7] и подмена клиентского SSL-сертификата. Рассмот- рим каждый в отдельности.

Атака *Bar Mitzvah* направлена на взлом алго- ритма симметричного шифрования RC4, который поддерживается протоколом TLS/DTLS. Для со- гласования параметров соединения в протоколе TLS/DTLS клиент и сервер обмениваются сообще- ниями ClientHello и ServerHello. Если в процессе согласования в качестве алгоритма симметричного шифрования будет выбран алгоритм RC4, то дан- ные, которые будут зашифрованы этим алгоритмом, могут быть расшифрованы. Для того чтобы избе- жать атаки данного типа, достаточно исключить возможность выбора алгоритма RC4 на этапе согла- сования параметров соединения.

Атака *Logjam* производится на сессионные ключи, которые устанавливаются во время обме- на по протоколу Диффи–Хеллмана с целью по- нижения их криптостойкости до 512-битных. Это возможно, если сервер поддерживает 512-битные ключи в протоколе Диффи–Хеллмана, используя специальный режим EXPORT\_DHE. Чтобы защи- титься от данной атаки, так же, как и в предыду- щем случае, достаточно корректно настроить сер- вер и отключить режим EXPORT\_DHE.

Атака *подмены клиентского SSL-сертифика- та (MITM).* Для осуществления атаки злоумыш- леннику необходимо каким-либо образом убедить жертву установить специально изготовленный клиентский SSL-сертификат, ключ от которого известен атакующему. В дальнейшем при согла- совании сессионного ключа по алгоритму Диф- фи–Хеллмана, зная секретный ключ клиента, зло- умышленник сможет вычислить сессионный ключ и нарушить конфиденциальность соединения. От данной атаки можно защититься, если использовать двухстороннюю аутентификацию.

*Node-to-Device.* Так как туманные вычисления мобильны, основной канал связи в большинстве случаев будет установлен с помощью соединения

Wi-Fi. Злоумышленник может прослушивать ка- нал связи, но нарушение конфиденциальности или целостности данных будет затруднено (если будут реализованы необходимые процедуры по защите соединения Wi-Fi и использованы прото- колы TLS/IPsec). Однако данный вид соединения будет подвержен атакам на физическом уровне, таким как исчерпание полосы пропускания и по- становка радиопомех, и ограничен дальностью связи Wi-Fi. При необходимости злоумышленник сможет забить радиочастотный канал связи и от- ключить пользователей от туманного узла. Если отказаться от Wi-Fi и перейти на технологии мо- бильной передачи данных 4G и потенциально 5G (в которых применяются технологии CDMA и ее развитие OFDMA), то это позволит противосто- ять атакам такого рода.

Для защиты первых двух типов соединений (Node-to-Cloud и Node-to-Node с использованием протоколов безопасности TLS/DTLS) достаточно корректной настройки сервера (настроить двух- стороннюю аутентификацию и отключить воз- можность выбора шифрования симметричным алгоритмом RC4 и режима EXPORT\_DHE).

Узким местом на данный момент в сетевой безопасности туманных вычислений является беспроводная передача данных с использованием Wi-Fi (Node-to-Device), из-за высокого риска по- явления угроз доступности сетевых узлов. Одним из возможных путей решения данной проблемы является переход на передачу данных с помощью мобильных сетей 4G (или 5G в будущем), в кото- рых применяются технологии CDMA и ее разви- тие OFDMA.

В данной статье была рассмотрена эталонная архитектура туманных вычислений, которую представил консорциум OpenFog.

Далее были рассмотрены существующие свя- зи в архитектуре туманных вычислений: Node-to- Cloud, Node-to-Node и Node-to-Device.

На основании анализа безопасности каждого вида связи были сделаны выводы об их уязвимо- стях и потенциальных методах защиты. Связи типа Node-to-Cloud и Node-to-Node могут быть уязвимы к атакам *Bar Mitzvah, Logjam* и *подмене клиентского SSL-сертификата.* Связь Node-to- Device будет наиболее уязвима к атакам на физи- ческом уровне.

Важно отметить, что для использования про- токола TLS/DTLS (соединения Node-to-Cloud и Node-to-Node) требуется разработка и внедрение в туманные вычисления инфраструктуры откры- тых ключей (PKI), поскольку PKI является необ- ходимой составляющей протокола TLS/DTLS. К сожалению, в представленной архитектуре этот вопрос не освещается, но можно предположить, что центры сертификации будут реализованы в ЦОДах, как наиболее доверенных элементах си- стемы, а каждый туманный узел будет иметь под-

писанный сертификат из ОВС, с помощью кото- рого можно будет реализовать аутентификацию. Кроме того, потребуется реализовать кроссерти- фикацию между ОВС, чтобы туманные узлы, ко- торые имеют сертификаты из разных ЦОДов, смогли построить цепочку доверия.

Дальнейшая работа будет посвящена модели- рованию связей между кончеными устройствами с использованием протокола ZeegBee и Wi-Fi для исследования сетевой безопасности связи Node- to-Device.

