Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1606

(09/2020)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность облачных вычислений –
Проектирование безопасности облачных вычислений

Требования к безопасности прикладной среды связи как услуги

Рекомендация МСЭ-Т X.1606

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределения реестра	X.1400–X.1429
Безопасность технологии распределения реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	**X.1602–X.1639**
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700–X.1729

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1606

Требования к безопасности прикладной среды связи как услуги

Резюме

В Рекомендации МСЭ-Т X.1606 определены угрозы безопасности и предлагаются требования к безопасности прикладной среды связи как услуги (CaaS). В настоящей Рекомендации описаны сценарии и функции CaaS с поддержкой многих видов связи. Затем определены конкретные угрозы, обусловленные уникальными функциями CaaS, и приведены рекомендации по соответствующим требованиям к безопасности CaaS.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1606	03.09.2020 г.	17-я	11.1002/1000/14265

Ключевые слова

Облачные вычисления, CaaS, требования к безопасности, риск.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

© ITU 2021

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1606

Требования к безопасности прикладной среды связи как услуги

1 Сфера применения

В настоящей Рекомендации основное внимание уделяется требованиям к безопасности прикладной среды связи как услуги (CaaS), которые отличаются от требований к безопасности программного обеспечения как услуги (SaaS), изложенных в [ITU-T X.1602]. CaaS организаций электросвязи соединяет в себе возможности связи с возможностями интернета. Такая конвергенция придает CaaS некоторые уникальные особенности, которые влекут за собой определенные риски. В настоящей Рекомендации определяются эти риски и предлагаются соответствующие требования безопасности.

Эти требования учитывают национальные правовые и нормативные обязательства, принятые в отдельных государствах-членах, где эксплуатируется CaaS. Данный текст основан на методике, приведенной в разделе 10 [ITU-T X.1601].

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений*.

[ITU-T X.1602] Рекомендация МСЭ-Т X.1602 (2016 г.), *Требования к безопасности прикладной среды программного обеспечения как услуги*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing – Framework and high-level requirements*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 аутентификация (authentication) [ITU-T X.1601]: Проверка идентичности пользователя, процесса или устройства, нередко являющаяся необходимым условием обеспечения возможности доступа к ресурсам информационной системы.

3.1.2 возможность (capability) [b-ISO 15531-1]: Свойство, заключающееся в способности выполнять данный вид деятельности.

3.1.3 облачные вычисления (cloud computing) [b-ITU-T Y.3500]: Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

ПРИМЕЧАНИЕ. – К примерам ресурсов относятся серверы, операционные системы, сети, программное обеспечение, приложения и оборудование для хранения.

3.1.4 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, которые активируются с помощью заявленного интерфейса.

3.1.5 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в деловых отношениях применительно к использованию облачных услуг.

ПРИМЕЧАНИЕ. – Деловые отношения необязательно предполагают наличие финансовых договоров.

3.1.6 партнер облачной услуги (cloud service partner) [b-ITU-T Y.3500]: Сторона, участвующая в поддержке деятельности либо поставщика облачной услуги, либо потребителя облачной услуги, либо обоих или же оказывает помощь в этой деятельности.

3.1.7 поставщик облачной услуги (cloud service provider) [b-ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

3.1.8 пользователь облачной услуги (cloud service user) [b-ITU-T Y.3500]: Лицо или действующий от его имени объект, которые связаны с потребителем облачной услуги и пользуются облачными услугами.

ПРИМЕЧАНИЕ. – К примерам таких объектов относятся устройства и приложения.

3.1.9 связь как услуга (communications as a service (CaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой возможностью, предоставляемой потребителю облачной услуги, является связь и взаимодействие в реальном времени.

ПРИМЕЧАНИЕ. – В CaaS могут предоставляться два типа возможностей: возможности платформы и возможности приложения.

3.1.10 режим с множеством арендаторов (multi-tenancy) [b-ITU-T Y.3500]: Распределение физических и виртуальных ресурсов, при котором несколько арендаторов и их вычисления и данные изолированы один от другого и недоступны друг другу.

3.1.11 оркестровка (orchestration) [b-ITU-T Y.3100]: В контексте IMT-2020 процессы, направленные на автоматизированную организацию, координацию, реализацию и использование сетевых функций и ресурсов как физической, так и виртуальной инфраструктуры по критериям оптимизации.

3.2.12 программное обеспечение как услуга (software as a service (SaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности приложения.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CaaS	Communications as a Service		Связь как услуга
CSC	Cloud Service Customer		Потребитель облачной услуги
CSN	Cloud Service Partner		Партнер облачной услуги
CSP	Cloud Service Provider		Поставщик облачной услуги
CSU	Cloud Service User		Пользователь облачной услуги
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
GSM	Global System for Mobile		Глобальная система подвижной связи
IAM	Identity and Access Management		Управление определением идентичности и доступом
IaaS	Infrastructure as a Service		Инфраструктура как услуга
ID	Identifier		Идентификатор
MMS	Multimedia Messaging Service		Услуга передачи мультимедийных сообщений
NaaS	Network as a Service		Сеть как услуга
OS	Operating System	ОС	Операционная система
PaaS	Platform as a Service		Платформа как услуга
PC	Personal Computer	ПК	Персональный компьютер

QR	Quick Response	Быстрый ответ
SaaS	Software as a Service	Программное обеспечение как услуга
SDK	Software Development Kit	Комплект инструментов разработки программного обеспечения
SIM	Subscriber Identity Module	Модуль идентификации абонента
SMS	Short Message Service	Услуга передачи коротких сообщений
URL	Uniform Resource Locator	Унифицированный указатель ресурса
(U)SIM	(Universal) Subscriber Identity Module	(Универсальный) модуль идентификации абонента
VoLTE	Voice over Long-Term Evolution	Передача голоса по сети LTE
VPN	Virtual Private Network	Виртуальная частная сеть

5 Соглашения

В настоящей Рекомендации не проводится различие между сервером и виртуальным сервером.

6 Обзор CaaS

Определение CaaS дано в пункте 3.1.9. В качестве общих требований к CaaS рекомендуются такие требования, как открытость возможностей связи, поддержка программного обеспечения связи и унифицированная связь (см. раздел 11 [ITU-T Y.3501]).

Согласно промышленной практике в системах CaaS обычно реализуются или поддерживаются следующие возможности:

– сочетание услуг электросвязи и интернета;
– связь в режиме реального времени;
– синхронизация нескольких устройств;
– изоляция ресурсов связи;
– обновление присутствия пользователя;
– групповой чат или собрание;
– встраивание в другие SaaS;
– поддержка режимов с требованием согласия пользователя и без него;
– настройка процесса обслуживания;
– обмен данными или файлами;
– управление определением идентичности и доступом (IAM).

Общая модель услуг CaaS показана на рисунке 1. На этом рисунке представлены четыре уровня – пользователи, доступ, услуги и ресурсы.

– На уровне пользователей находятся терминалы пользователей облачных услуг (CSU), которые могут выполнять определенные клиентские программы CaaS и могут иметь доступ в интернет и даже к сетям электросвязи.
– На уровне доступа представлены туннели различных типов, обычно предоставляющие терминалу доступ к целевой услуге CaaS.
– Уровень услуг, который также представляет собой уровень CaaS, принадлежит поставщику облачных услуг (CSP), который для реализации услуг опирается на необходимые внутренние и внешние ресурсы. Уровень услуг настраивает процессы обслуживания и выделяет ресурсы потребителям облачных услуг (CSC), поддерживает (виртуальную) динамическую сеть обслуживания потребителей облачных услуг со своими CSU и изолирует вычислительные ресурсы и сети связи каждого CSC.

– Уровень ресурсов предоставляет ресурсы базовой инфраструктуры, относящиеся к обработке данных и связи, в состав которой могут входить инфраструктура как услуга (IaaS), платформа как услуга (PaaS) и сеть как услуга (NaaS).

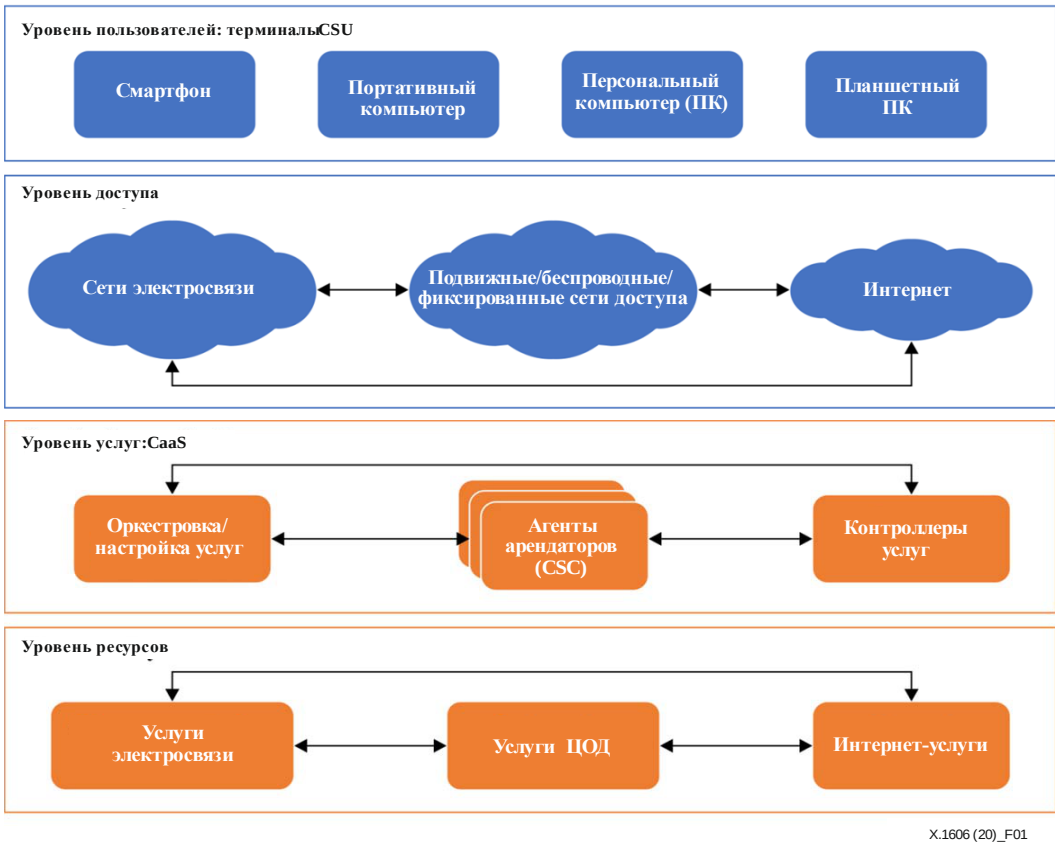

Рисунок 1 − Общая модель услуг CaaS

В остальной части настоящей Рекомендации:

– раздел 7 посвящен анализу угроз безопасности для CaaS, направленных на один или несколько из четырех уровней;

– раздел 8 содержит рекомендуемые требования к безопасности для CaaS, направленные на предотвращение угроз на трех уровнях:

- на уровне терминалов CSU;
- на уровне CaaS;
- на уровне ресурсов обслуживания.

Уровень доступа здесь не рассматривается, поскольку его возможности по обеспечению безопасности не контролируются CaaS, хотя оператор CaaS и CSU могут оценивать или контролировать степень безопасности уровня доступа.

7 Угрозы безопасности для CaaS

Угрозы и проблемы безопасности облачных вычислений, определенные в [ITU-T X.1601] (а также перечисленные в Дополнении I), могут относиться к различным сценариям CaaS. Кроме того, некоторые конкретные угрозы для CaaS указаны в пунктах 7.1–7.8.

7.1 Угрозы, связанные с идентичностью

Ядром CaaS служат возможности унифицированной связи, которые несколько отличаются от возможностей других SaaS. Используя облачные вычисления, CaaS интегрирует и расширяет

возможности связи между терминалами. CaaS поддерживает большинство основных типов терминалов или операционных систем (ОС), таких как смартфоны и персональные компьютеры (ПК).

Следовательно, в случае нарушения идентичности в рамках модели связи многих пунктов со многими пунктами CaaS может сталкиваться с некоторыми особыми угрозами.

7.1.1 Кража регистрационных идентификационных данных

Для удобства CSU во многих системах CaaS используется решение аутентификации, поддерживающее аутентификацию по номеру мобильного телефона (то есть мобильному ID), по имени пользователя и паролю или оба вида аутентификации. В этом случае решение может быть настроено так, что именем пользователя по умолчанию служит мобильный ID. Кроме того, некоторые системы CaaS поддерживают возможность доступа к услуге для одного CSU с одним идентификатором с нескольких терминалов одновременно или синхронизацию истории сообщений между несколькими терминалами.

Безопасность аутентификации по номеру мобильного телефона в значительной степени зависит от надежности средств аутентификации и шифрования оператора сети подвижной связи и (универсального) модуля идентификации абонента (U)(SIM-карты), в котором хранятся регистрационные данные. Некоторые (доказанные на практике) уязвимости, имеющие место в сетях подвижной связи, особенно в сетях GSMA (Global System for Mobile Communications Alliance), ослабляют эту надежность и могут привести к перехвату (временному) регистрационных идентификационных данных. Например, модули идентификации абонента (SIM-карты) некоторых типов можно физически дублировать, а некоторые коды динамической аутентификации, передаваемые через услугу передачи коротких сообщений (SMS) в глобальной системе подвижной связи (GSM), можно перехватить. Для временного незаметного взлома идентификатора также могут быть использованы перехваченные временные ключи шифрования.

Кроме того, аутентификация по имени пользователя и паролю может использовать этот тип аутентификации для (одновременного) наблюдения за CSU с других подходящих терминалов. Например, если злоумышленнику удастся получить доступ к мобильному терминалу CSU с (U)SIM-картой или регистрационными данными виртуальной SIM-карты, он может считать имя пользователя из буферной памяти и применить механизм сброса пароля, сохранив новый пароль в буферной памяти терминала. CSU может не заметить, что пароль был сброшен, и тогда злоумышленник сможет тайно контролировать текущую переписку и даже ее историю.

7.1.2 Подделка идентичности

Как только регистрационные идентификационные данные пользователя облачных услуг (CSU) попали в руки злоумышленника, тот может использовать их для доступа к услугам CSC, с которым связан этот CSU. В то же время злоумышленник может заполучить соответствующие данные социального субъекта с регистрационными идентификационными данными CSU или даже подделать существующего или нового социального субъекта, который сначала будет продемонстрирован функцией присутствия.

Присутствие – это один из общих элементов CaaS, который обычно служит "автопортретом" CSU и содержит его миниатюрное изображение и некий короткий текст. Благодаря присутствию CSU может быстро узнавать других CSU, относящихся к тому же CSC. Однако такое присутствие можно сфальсифицировать с помощью подложной идентичности и использовать в мошеннических целях. Например, сфальсифицировав присутствие в качестве члена правления, злоумышленник может получить от бухгалтера конфиденциальные финансовые данные компании.

Стандартной конфигурацией CaaS может быть видеочат в реальном времени. Для усиления впечатления подлинности личности (социального субъекта) и мошеннической деятельности может быть сфальсифицирована сцена, демонстрируемая злоумышленником посредством видеопотока.

7.2 Угрозы, связанные с управлением жизненным циклом учетной записи

CSU, CSC или CSP могут иметь право потребовать удаления учетной записи, на которую у них есть полномочия. Когда в общем жизненном цикле учетной записи требуется ее удалить, должно быть заранее согласовано, что должен делать CSP в отношении контента и информации учетной записи, распространенных по всей услуге CaaS, и может ли CSC хранить эти данные в своем логическом пространстве, а CSU – в своем терминале.

При списании или краже терминала вся информация учетной записи и любые связанные с ней данные должны удаляться из буферной памяти.

7.3 Угроза, связанная с оркестровкой

С помощью функции оркестровки (см. [b-ITU-T Y.3100]) CSC может настраивать процессы предоставления своих услуг и возможности своих услуг самостоятельно либо через своего CSP. Например, CSC может настроить процесс и преимущественное право управления членством в чат-группе, а также расширить или сузить границы, в которых CSU разрешено искать партнеров.

Что касается требований к потребителям, то CSP может позволить нескольким CSC обмениваться контактной информацией и даже общаться напрямую, а также укрупнять CSC, объединяя их друг с другом.

Кроме того, для реализации новых услуг CSP может ужесточать или ослаблять предварительные условия по обеспечению безопасности в сети, к которой у CSU есть доступ.

Любая оркестровка без полного учета безопасности может негативно повлиять на изоляцию информации и услуг. Например, если система CaaS CSC оркестрована для интеграции услуг голосовой связи и передачи сообщений в сети GSM, то обеспечить полную изоляцию практически невозможно, поскольку объекты сети GSM применяют технологии ранних поколений и не могут поддерживать никакие функции изоляции. Если для более гибкой поддержки услуг оркестровкой будет разрешен небезопасный тип сети, то это может повысить уровень риска для CaaS больше, чем просто какой-нибудь CSC. Например, если для обеспечения качества видеочата в CaaS требование доступа через виртуальную частную сеть (VPN) в качестве метода изоляции переквалифицировано из обязательного в необязательное, то возрастет риск перехвата.

7.4 Угроза, связанная с контекстом терминалов

Контекст безопасности терминалов в CaaS может быть неопределенным, особенно когда терминалами являются смартфоны или портативные устройства. Если эти терминалы находятся в личной собственности, то контекст безопасности может быть более сложным. Такие терминалы могут использоваться родственниками или гостями CSU. Экран терминала может проецироваться на другой экран или использоваться совместно с другим экраном, так что возможна запись изображения на экране без ведома пользователя. В незащищенной сети злоумышленникам легче выявить уязвимости терминала. Передаваемый через CaaS контент может быть незашифрованным и храниться в терминале. Каждый из этих случаев может привести к утечке данных.

Если злоумышленник получает возможность управлять терминалом (удаленно или локально), он может использовать этот терминал для эксплуатации уязвимостей CaaS и даже соответствующих CSU. Управляя одновременно множеством терминалов, организованных в бот-сеть, злоумышленник также может инициировать распределенную атаку типа отказ в обслуживании (DDoS).

7.5 Угроза спама и распространение вредоносных программ

CSU может подвергаться дополнительной нагрузке или даже фишингу из-за спам-атак со стороны других CSU через CaaS. Действительно, в большинстве случаев CSU трудно рационально определить, можно ли доверять информации того или иного короткого унифицированного указателя информационных ресурсов (URL) или кода быстрого ответа (QR), что может привести к попаданию CSU на фишинговый веб-сайт или загрузке вредоносной программы.

7.6 Угроза со стороны расширений

Вполне естественно, что CaaS предоставляет те или иные расширения, основанные на ее базовых услугах, таких как обмен файлами, встроенный веб-браузер, система управления контентом и даже электронный бизнес. В большинстве случаев это довольно легкие расширения.

Уязвимости этих расширений могут создавать значительную угрозу для самой CaaS. Например, щелкнув на незащищенном коротком URL, можно задействовать расширения веб-браузера, не имеющие защиты от опасных веб-адресов, так что значительно возрастает вероятность нарушения безопасности CSU и даже CaaS.

Некоторые расширения могут спровоцировать CSU выйти из своей текущей услуги CaaS и перейти в другую, мошенническую услугу. Если CSU не заметит такого перехода, он не сможет должным образом и своевременно отреагировать, что приведет к значительному разнообразному ущербу (использованию большего количества уязвимостей, вымогательству, в том числе с помощью программ-вымогателей, и т. д.).

7.7 Угрозы, связанные с комплектом инструментов разработки программного обеспечения

CaaS может предоставлять комплект инструментов разработки программного обеспечения (SDK), чтобы стимулировать интеграцию других приложений или SaaS. Интеграция, как правило, предполагает некоторую степень доверия между CaaS и пользователями SDK. Следовательно, уязвимости пользователя SDK могут усилить угрозу атаки или злоумышленного использования CaaS.

Поскольку терминал может иметь несколько регистрационных идентификационных данных для разных CSC, пользователь SDK CaaS может использовать эти регистрационные данные без разрешения для получения несанкционированного доступа к другим CSC.

7.8 Угрозы из-за уязвимостей сетей электросвязи

Если CaaS, кроме доступа в интернет, поддерживает другие возможности оператора сети электросвязи, такие как SMS, передача голоса по сети LTE (VoLTE), коммутация каналов, передача мультимедийных сообщений (MMS) и определение местоположения, то безопасность сети электросвязи может оказывать прямое влияние на CaaS.

Любое удавшееся использование уязвимостей сети электросвязи может привести к утечке данных CaaS. Точно так же любая успешная атака на сеть электросвязи, особенно на узлы, соединенные с серверами CaaS, может расширить незащищенное пространство CaaS.

Более того, поскольку современные имеющиеся на рынке терминалы способны активно переключаться между сетями доступа и VPN различных поставщиков услуг в соответствии с заранее определенной политикой, обращая мало внимания на степень доверия к сети доступа и ее подлинность, CSU может использовать небезопасную сетевую среду, не догадываясь об этом, что чревато утечкой конфиденциальной информации.

8 Требования к безопасности CaaS

К сценариям CaaS применяются требования к безопасности SaaS, определенные в [ITU-T X.1602]. Кроме того, в этом разделе установлены некоторые дополнительные требования к безопасности для предотвращения угроз, перечисленных в разделе 7.

8.1 Управление определением идентичности и доступом

8.1.1 Управление определением идентичности

Оператору CaaS следует установить верхний предел количества терминалов, которым разрешено одновременно использовать одни и те же регистрационные идентификационные данные. Он может утвердить один терминал с необходимыми идентификаторами оборудования и услуг в качестве основного контроллера, который будет разрешать доступ другим терминалам по требованию.

Оператор CaaS может контролировать параллельные терминалы с одинаковыми регистрационными идентификационными данными и информировать все терминалы (или по крайней мере первичный контроллер) о последнем статусе других параллельных терминалов. CSU может использовать первичный контроллер или прохождение более надежной аутентификации (такой, как обходная аутентификация), чтобы заставить определенный терминал выйти из сети, запретить ему любой доступ в будущем и даже удалить оставшуюся в нем информацию.

Оператор CaaS может рассмотреть вопрос о принуждении CSU использовать разные регистрационные данные (или по крайней мере разные пароли) для разных CSC, что может понизить риск использования одного украденного набора регистрационных данных для доступа ко многим CSC.

8.1.2 Управление доступом

Если для CaaS применяются параллельные терминалы с одними и теми же регистрационными идентификационными данными, то целесообразно позволить CaaS получать и обновлять сведения о географическом местоположении терминалов, чтобы можно было обнаруживать любые аномалии доступа к терминалу. Поскольку один терминал может получать доступ ко многим сетям одновременно, CaaS может рассмотреть возможность использования многомерной информации для перекрестной проверки подлинности местоположения.

Если безопасность сети не может быть гарантирована, то хорошим выбором для повышения безопасности инфраструктуры может быть VPN. CaaS следует рассмотреть вопрос о требовании, чтобы CSU или CSC использовали обязательную услугу VPN, и запретить CSU или CSC принимать любые другие услуги VPN в качестве промежуточного средства доступа к обязательной услуге VPN. Необязательная или ненадежная VPN может скрывать местоположение терминала, а также увеличивает риск атаки через посредника.

Кроме того, если CSC не может принять риск перехвата SMS GSM, то CaaS следует рассмотреть возможность контроля типа сети, к которой обращается любой CSU, и отказаться от использования SMS в качестве метода аутентификации в случае нахождения CSU в сети GSM. Как вариант, CaaS может просто исключить ресурс SMS GSM для CSC.

8.1.3 Проверка идентичности

Поскольку для создания "автопортрета" CSU может использовать малопонятную, неточную или даже фальсифицированную информацию, CaaS следует информировать всех CSU, проверена ли социальная идентичность их партнеров какой-либо доверенной третьей стороной. Этой третьей стороной может быть CSC, CaaS или любой другой независимый орган. Проверка может быть обязательной или необязательной, но если она необязательна, то, возможно, потребуется предупреждать CSU о том, что CSP или CSC не несут ответственности за подлинность социальной идентичности CSC.

Поскольку социальная или деловая идентичность CSC, когда-то ставшего клиентом CaaS, может разительно отличаться от той, что представлена публично, оператору CaaS рекомендуется рассмотреть возможность сравнения публично заявленной идентичности CSC с доступной ему информацией во избежание возможного обмана общественности или мошенничества в деловой сфере. Например, злонамеренный CSC может выдать себя за благотворительную организацию и собирать пожертвования на какие-нибудь фальшивые цели, обманывая CSU.

8.1.4 Управление учетными записями

Поскольку CSU может иметь по меньшей мере одну учетную запись у CSC, а CSC также может иметь по крайней мере одну учетную запись CaaS, оператор CaaS должен предоставить CSU или CSC все права доступа к данным своей учетной записи в соответствии с правом собственности в отношении данных. Кроме того, когда учетную запись нужно аннулировать или удалить, оператор CaaS должен предоставить возможность надежного физического уничтожения данных учетной записи в терминале, услуге и сети в соответствии с юридическими условиями, установленными владельцем данных.

8.2 Безопасность терминала

8.2.1 Внутренняя безопасность

Оператору CaaS следует обеспечить технические меры, такие как инструментарий безопасности или модуль безопасности, встроенный в терминалы CSU, для проведения периодических проверок безопасности или проверок по требованию. Проверка безопасности позволит оценить, удовлетворяет ли контекст терминала CSU обязательным требованиям к безопасности, прежде чем предоставить ему доступ к CaaS. Если терминал CSU не прошел проверку безопасности, оператор CaaS может рассмотреть вопрос об отказе в предоставлении услуг (частичном). В то же время оператору CaaS следует давать CSU рекомендации по устранению выявленных рисков безопасности или непосредственно устранять уязвимости CSU с его разрешения.

8.2.2 Внешняя безопасность

Программное обеспечение, используемое в терминалах CSU, должно предоставляться оператором CaaS. Оператору CaaS также следует предоставить безопасную платформу распределения или

источники программного обеспечения, которые должны быть официальными или авторизованными. Оператору CaaS также следует указать механизм верификации, чтобы терминалы CSU могли использовать его для проверки подлинности и целостности ПО перед обновлением. В ОС или самом программном обеспечении терминалов CSU должна быть предусмотрена возможность отката в том случае, если обновление не работает.

В большинстве случаев обновление безопасности программного обеспечения терминала факультативно. Однако если какая-либо уязвимость может привести к значительному ущербу для CaaS, CSC или даже других CSU и обновление безопасности программного обеспечения терминала устраняет эту уязвимость, CaaS может рассмотреть возможность временного отказа в доступе к услугам для терминалов CSU до их успешного обновления в соответствии с пользовательским соглашением.

В большинстве случаев распределение программного обеспечения терминала CaaS является открытым. Тем не менее в отдельных случаях CSC может потребовать применения специального программного обеспечение терминала и ограничить сферу его распределения, например, только персоналом CSC. Тогда распределение следует сделать закрытым и перед загрузкой или обновлением программного обеспечения требовать двустороннюю аутентификацию CSU и CaaS.

8.3 Безопасность услуг

8.3.1 Безопасность оркестровки

Перед развертыванием или настройкой изменений, связанных с оркестровкой, необходимо оценить, может ли это изменение повлиять на границы безопасности, понизить уровень безопасности или нарушить доверительные отношения. Если возможны те или иные негативные последствия, то CSP, CSC и даже CSU должны пересмотреть и согласовать требования к безопасности или соглашения с CaaS.

8.3.2 Противодействие спаму

Оператору CaaS следует рассмотреть вопрос о поддержке функции противодействия спаму в качестве дополнительной возможности для CSC. CSP может также рассмотреть возможность разрешения CSC включать в свой механизм CaaS стороннюю функцию противодействия спаму. Разные соглашения о предоставлении услуг и пользовательские соглашения между CSP, CSC и CSU могут налагать разные ограничения на использование функции противодействия спаму.

Например, если все CSU являются сотрудниками CSC и соответствующий механизм CaaS используется исключительно в интересах CSC, то возможно, что для использования функции противодействия спаму достаточно соглашения между CSP и CSC.

Если же некоторые CSU являются клиентами CSC, то потребуется, чтобы эти CSU разрешили CSC (вместе с CSP) помогать им в противодействии спаму.

В общем случае функция противодействия спаму должна находиться на стороне терминала, на стороне облака или и там и там. Об альтернативных технологиях, используемых в этой функции, см. [b-ITU-T X.1244] и [b-ITU-T X.1246].

8.4 Координация мер безопасности

8.4.1 Безопасность расширений и SDK

Оператору CaaS следует допускать только те расширения, которые прошли проверку безопасности в его услуге. Программное обеспечение терминала должно помогать CaaS контролировать и анализировать любые аномалии расширений. Белый список поможет CaaS ограничить возможность доступа расширений к внешним ссылкам или именам доменов.

Если для предоставления услуги расширению необходим доступ к данным клиента, то предварительным условием должно быть явное разрешение CSU. Для последующего аудита будет полезна четкая запись об обращении к данным клиента.

SDK для CaaS должен иметь возможность отслеживать и анализировать аномалии приложений или SaaS, содержащего SDK. SDK должен шифровать и изолировать регистрационные идентификационные данные во избежание возможных злоупотреблений. Например, приложение A и приложение B могут

содержать один и тот же SDK и работать в одном и том же терминале, но ни одно из них не может получить доступ к регистрационным идентификационным данным другого.

8.4.2 Инфраструктура безопасности

Оператор CaaS должен знать об угрозах со стороны инфраструктуры, например если он интегрирует услуги сетей электросвязи, такие как SMS и голосовой вызов. Оператор CaaS должен рассмотреть возможность установки шлюза между его услугой и сетями электросвязи для контроля, противодействия или фильтрации возможного спама и мошенничества с использованием услуг электросвязи. Целесообразно, чтобы оператор CaaS мог информировать CSU о типах используемых каналов связи или услуг.

Дополнение I

Краткий перечень угроз и проблем безопасности, указанных в Рекомендации МСЭ-Т X.1601

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Как упоминалось в разделе 7, угрозы и проблемы безопасности облачных вычислений, определенные в [ITU-T X.1601], могут относиться к различным сценариям CaaS. В данном Дополнении перечислены все угрозы и проблемы безопасности, указанные в [ITU-T X.1601], для быстрой проверки. Если требуется более подробная информация, см. [ITU-T X.1601].

– Угрозы безопасности облачных вычислений
  a) Угрозы безопасности для потребителей облачных услуг (CSC)
    1) Потеря и утечка данных
    2) Незащищенный доступ к услуге
    3) Внутренние угрозы
  b) Угрозы безопасности для поставщиков облачных услуг (CSP)
    1) Несанкционированный административный доступ
    2) Внутренние угрозы
– Проблемы безопасности облачных вычислений
  a) Проблемы безопасности для потребителей облачных услуг (CSC)
    1) Неопределенность в отношении ответственности
    2) Потеря доверия
    3) Потеря управления
    4) Потеря конфиденциальности
    5) Неготовность услуги
    6) Привязка к одному CSP
    7) Неправомерное присвоение интеллектуальной собственности
    8) Потеря целостности программного обеспечения
  b) Проблемы безопасности для поставщиков облачных услуг (CSP)
    1) Неопределенность в отношении ответственности
    2) Совместно используемая среда
    3) Несогласованность и конфликт механизмов защиты
    4) Конфликт юрисдикций
    5) Риски, связанные с изменениями
    6) Неудачный переход и интеграция
    7) Перебои в деятельности
    8) Привязка к партнеру облачной услуги (CSN)
    9) Уязвимость цепи поставок
    10) Взаимозависимость программного обеспечения
  c) Проблемы безопасности для партнеров облачной услуги (CSN)
    1) Неопределенность в отношении ответственности
    2) Неправомерное присвоение интеллектуальной собственности
    3) Потеря целостности программного обеспечения

Дополнение II

Сопоставление угроз и требований безопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении угрозы, перечисленные в разделе 7, сопоставляются с требованиями, перечисленными в разделе 8 (см. таблицу I.1).

Таблица I.1 − Сопоставление угроз безопасности с проблемами безопасности, указанными в настоящей Рекомендации

Угрозы, указанные в разделе 7	**Соответствующие требования, указанные в разделе 8**
7.1 Угрозы, связанные с идентичностью	8.1 Управление определением идентичности и доступом
7.1.1 Кража регистрационных идентификационных данных	8.1.1 Управление определением идентичности 8.1.2 Управление доступом 8.1.4 Управление учетными записями
7.1.2 Подделка идентичности	8.1.3 Проверка идентичности 8.1.4 Управление учетными записями
7.2 Угрозы, связанные с управлением жизненным циклом учетной записи	8.1.4 Управление учетными записями
7.3 Угроза, связанная с оркестровкой	8.3.1 Безопасность оркестровки
7.4 Угроза, связанная с контекстом терминалов	8.2 Безопасность терминала
7.5 Угроза спама и распространение вредоносных программ	8.2 Безопасность терминала 8.3.2 Противодействие спаму
7.6 Угроза со стороны расширений	8.4.1 Безопасность расширений и SDK
7.7 Угрозы, связанные с комплектом инструментов разработки программного обеспечения	8.4.1 Безопасность расширений и SDK
7.8 Угрозы из-за уязвимостей сети электросвязи	8.4.2 Инфраструктура безопасности

Библиография

[b-ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 год), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях*.

[b-ITU-T X.1246] Рекомендация МСЭ-Т X.1246 (2015 год), *Технологии, используемые в организациях электросвязи для противодействия голосовому спаму*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 год) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология.*

[b-ISO 15531-1] ISO 15531-1:2004, *Industrial automation systems and integration – Industrial manufacturing management data – Part 1: General overview*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2021 г.