Международный союз электросвязи

МСЭ-Т X.1127

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2017)

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

Безопасные приложения и услуги – Безопасность подвижной связи

Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов

Рекомендация МСЭ-Т X.1127

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	
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	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	
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 системы (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Протоколы безопасности	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

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

Рекомендация МСЭ-Т X.1127

Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов

Резюме

Рекомендация МСЭ-Т X.1127 посвящена функциональным требованиям безопасности и функциональной архитектуре механизмов противодействия кражам смартфонов, которые базируются на общих требованиях, сформулированных GSMA.

Количество смартфонов быстро растет, и они стали практически неотъемлемой частью повседневной жизни. К сожалению, у большого числа пользователей смартфоны похищаются. Мера противодействия кражам смартфонов, то есть система блокирования (kill switch), предназначенная для использования в случае утери или кражи смартфона, должна обеспечивать следующие возможности:

– дистанционное удаление хранящихся в смартфоне данных авторизованного пользователя;

– приведение смартфона в неработоспособное состояние для неавторизованного пользователя;

– предотвращение возможности возобновления его работы без разрешения авторизованного пользователя, насколько это технически возможно;

– возвращение смартфона в рабочее состояние авторизованным пользователем и, по возможности, восстановление хранившихся в нем пользовательских данных.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1127	06.09.2017 г.	17-я	11.1002/1000/13259

Ключевые слова

Меры противодействия кражам, мобильный телефон, требования безопасности.

* 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 с целью 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/.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т X.1127

Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов

1 Сфера применения

В настоящей Рекомендации рассматриваются функциональные требования безопасности и функциональная архитектура для меры противодействия кражам смартфонов (то есть блокирование "kill switch"), которая дает пользователям возможность дистанционно удалять свои личные данные или блокировать украденный или утерянный смартфон.

Предполагается, что функциональные требования безопасности и функциональная архитектура, определенные в настоящей Рекомендации, применимы к смартфонам, способным обеспечить меры противодействия кражам, отражающие желания владельцев смартфонов, производителей смартфонов и операторов подвижной связи.

В настоящей Рекомендации основное внимание уделяется функциональным требованиям, функциональной архитектуре и механизмам противодействия кражам. В ней используется эталонная модель, включающая владельца устройства, авторизованный сервер, сервер резервирования и утерянные или украденные устройства. Угрозы, специфичные для мер противодействия кражам, описаны в Дополнении III. Настоящая Рекомендация не изменяет общих требований к функциям противокражной защиты смартфонов, которые разработаны GSMA [b-GSMA].

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.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 очистка данных (data sanitization) [b-NIST SP 800-88]: Меры, принимаемые для того, чтобы сделать данные, записанные на носителе информации, невосстановимыми как обычными, так и чрезвычайными средствами.

3.1.2 гарантия аутентификации объекта (entity authentication assurance) (EAA) [ITU-T X.1254]: Степень достигаемой в процессе аутентификации уверенности в том, что объект является тем, которым, как он утверждает, является, или тем, которым, как ожидается, он является (это определение основывается на определении "гарантия аутентификации", данном в [b-ITU-T X.1252]).

ПРИМЕЧАНИЕ. – Эта уверенность основывается на степени доверия к связи между объектом и представленной идентичностью.

3.1.3 идентичность (identity) [b-ITU-T X.1250]: Представление объекта в виде одного или более информативных элементов, которые позволяет объекту или объектам быть в достаточной мере отличимыми в пределах контекста. Для задач IdM термин "идентичность" понимается как контекстуальная идентичность (поднабор атрибутов), то есть разнообразие атрибутов ограничено

структурой с определенными граничными условиями (контекстом), в которой этот объект существует и взаимодействует.

ПРИМЕЧАНИЕ. – Каждый объект выражается одной целостной идентичностью, которая объединяет все возможные информативные элементы, характеризующие эту идентичность (атрибуты). Однако эта целостная идентичность является теоретическим объектом и не поддается никакому описанию и практическому применению, так как количество всех возможных атрибутов неопределимо.

3.1.4 блокирование "kill switch" (kill switch) [b-GSMA]: Способ блокирования важных функций мобильного устройства.

ПРИМЕЧАНИЕ. – По существу это функция, встроенная в мобильное устройство, при инициировании которой, например путем передачи в мобильное устройство сообщения определенного формата, устройство прекращает работу в соответствии со своим назначением, и его работа (или использование) может быть восстановлена только с разрешения владельца этого устройства.

3.1.5 мобильный телефон (mobile phone) [b-ITU-T X-Sup.19]: Электронное устройство, используемое для осуществления телефонных вызовов и отправки текстовых сообщений на обширной территории с помощью радиодоступа к сетям подвижной связи общего пользования и при этом обеспечивающее мобильность пользователя.

3.1.6 смартфон (smartphone) [b-ITU-T X-Sup.19]: Мобильный телефон с большими вычислительными возможностями, поддержкой различных типов соединений и усовершенствованной операционной системой, предоставляющей платформу для сторонних приложений.

3.1.7 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.1.8 туннель (tunnel) [b-ISO/IEC 27033-1]: Тракт данных между устройствами, объединенными в сеть, который создается через существующую сетевую инфраструктуру.

ПРИМЕЧАНИЕ. – Туннели могут создаваться с использованием таких методов, как инкапсуляция протокола, коммутация по меткам или виртуальные каналы.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 аппаратное обеспечение устройства (device hardware): Физические компоненты, которые в совокупности обеспечивают функционирование мобильного устройства, включая экран, клавиши, печатную плату, микросхемы, SIM-карту, сменное ЗУ и т. д.

3.2.2 программное обеспечение устройства (device software): Все программы, записанные в устройстве и на SIM-карте, включая приложения, операционную систему, загрузчик, загрузочное ПЗУ и прошивку.

3.2.3 пользователь устройства (device user): Авторизованный пользователь мобильного устройства.

3.2.4 безопасное туннелирование (secure tunneling): Протокол, который обеспечивает безопасную передачу данных или сообщений из одного пункта сети в другой.

ПРИМЕЧАНИЕ. – Безопасное туннелирование обычно поддерживает аутентификацию объектов, целостность сообщений и конфиденциальность сообщений.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ATM	Automated Teller Machine	Банкомат
CRL	Certificate Revocation List	Список аннулированных сертификатов
DER	Distinguished Encoding Rules	Отличительные правила кодирования
DDoS	Distributed Denial-of-Service	Распределенная атака типа "отказ в обслуживании"
DM	Device Management	Управление устройством
EAA	Entity Authentication Assurance	Гарантия аутентификации объекта

GPS	Global Positioning System	Глобальная система определения местоположения
GSMA	Groupe Speciale Mobile Association	Всемирная ассоциация операторов подвижной связи
HTTP	Hyper-Text Transfer Protocol	Протокол передачи гипертекста
LoA	Level of Assurance	Уровень гарантии
MAC	Message Authentication Code	Код аутентификации сообщения
OCSP	Online Certificate Status Protocol	Онлайновый протокол статуса сертификата
OMA	Open Mobile Alliance	Открытый альянс подвижной связи
OTP	One-Time Password	Одноразовый пароль
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PKI	Public-Key Infrastructure	Инфраструктура открытых ключей
SIM	Subscriber Identity Module	Модуль идентификации абонента
SMS-SC	Short Message Service – Service Centre	Центр передачи коротких сообщений
SSL	Secure Socket Layer	Протокол защищенных сокетов
TCP	Transmission Control Protocol	Протокол управления передачей
TFA	Three-Factor Authentication	Трехфакторная аутентификация
TLS	Transport Layer Security	Безопасность транспортного уровня
U	Universal	Универсальный
UICC	Universal Integrated Circuit Card	Универсальная карта с интегральной схемой
USSD	Unstructured Supplementary Service Data	Неструктурированные данные дополнительных услуг
2FA	2-Factor Authentication	Двухфакторная аутентификация

5 Соглашения по терминологии

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) "должен" – обозначает требование;

b) "следует" – обозначает рекомендацию;

c) "разрешается" – обозначает разрешение;

d) "может" – обозначает возможность и способность.

6 Обзор мер противодействия кражам

6.1 Меры противодействия кражам

Количество смартфонов быстро растет, и они стали неотъемлемой частью повседневной жизни. Однако у миллионов пользователей смартфонов они были украдены. Мера противодействия кражам смартфонов, то есть система блокирования "kill switch", должна обеспечивать следующие возможности:

– дистанционное удаление хранящихся в смартфоне личных данных пользователя в случае его утери или кражи;

– приведение смартфона в неработоспособное состояние для неавторизованного пользователя;

– сохранение, при необходимости, личных данных пользователя на сервере резервирования, управляемом оператором сотовой сети или производителем устройства;

– предотвращение возможности возобновления его работы без разрешения авторизованного пользователя;

– возвращение смартфона в рабочее состояние авторизованным пользователем и, по возможности, восстановление хранившихся в нем личных данных пользователя.

Программное обеспечение для противокражной защиты, установленное на мобильном устройстве, позволяет заблокировать украденный или утерянный телефон.

Существует два сценария запуска функций блокирования, когда владельцу мобильного устройства становится известно, что оно утеряно или украдено:

1) владелец устройства обращается к своему оператору сотовой связи, который передает в мобильное устройство команду блокирования;

2) владелец устройства запускает приложение на другом мобильном устройстве или осуществляет доступ к системе блокирования, которая приводит утерянное/украденное мобильное устройство в нерабочее состояние.

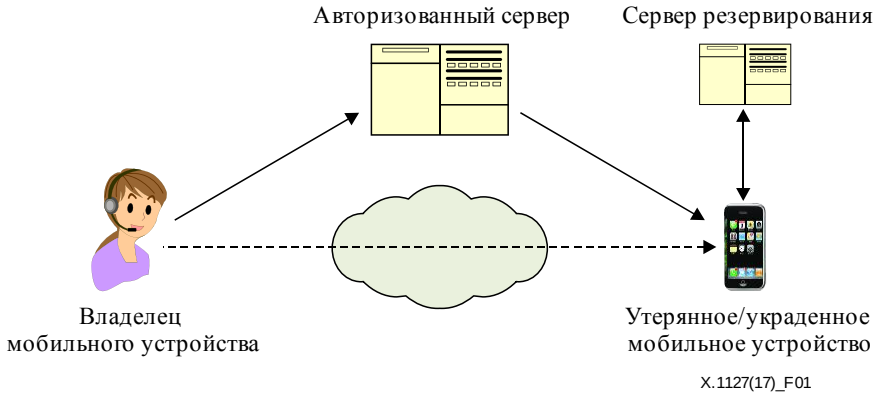


Рисунок 1 − Эталонная модель для мер противодействия кражам

На рисунке 1 представлена эталонная модель для мер противодействия кражам мобильных устройств. Авторизованный сервер поддерживает функцию блокирования украденных или утерянных мобильных устройств и управляется поставщиком услуг сотовой связи или производителями устройств. Авторизованный сервер направляет в украденное/утерянное мобильное устройство команду блокирования. По требованию владельца устройства сервер резервирования восстанавливает личные данные с мобильного устройства.

Связь между утерянным/украденным мобильным устройством и авторизованным сервером должна быть защищена с использованием безопасного туннеля (например, на основе протокола защищенных сокетов (SSL)). Связь между утерянным/украденным мобильным устройством и сервером резервирования также должна быть защищена с использованием безопасного туннеля (например, SSL).

Настоящая Рекомендация основана на структуре гарантии аутентификации объекта (EAA) для управления EAA, которая описана в [ITU-T X.1254]. В этой структуре EAA определены четыре уровня гарантии (LoA) аутентификации объекта. Каждый LoA описывает степень уверенности в процессах, приводящих к аутентификации, включая сам процесс аутентификации, обеспечивая таким образом гарантию того, что объект, использующий конкретную идентичность, является тем самым объектом, которому эта идентичность была присвоена.

В некоторых юрисдикциях может требоваться установка программного обеспечения для противокражной защиты или обеспечение его доступности для загрузки (скачивания). Так в Соединенных Штатах в штате Калифорния в настоящее время действует обязательное требование об установке противокражного программного обеспечения на новые телефоны, но при этом пользователи имеют возможность отключить функцию противокражной защиты, хотя по умолчанию она будет включена. Управление такой функцией осуществляется путем отказа, а не разрешения, поэтому ожидается, что большинство владельцев мобильных устройств будут использовать меры противодействия кражам и, следовательно, вероятность того, что любое данное мобильное устройство защищено, будет намного выше.

6.2 Требования высокого уровня, предъявляемые к мерам противодействия кражам

При передаче сообщений, связанных с противодействием кражам, из авторизованного сервера в мобильное устройство предъявляются следующие требования безопасности высокого уровня:

– аутентификация объекта;
– целостность сообщения;
– обнаружение повторной передачи и целостность последовательности;
– подтверждение получения и исполнения;
– конфиденциальность сообщений;
– указание используемых механизмов безопасности.

7 Функциональная архитектура для мер противодействия кражам мобильных телефонов

7.1 Угрозы, касающиеся мер противодействия кражам мобильных телефонов

В этом пункте описывается ряд выявленных угроз безопасности, затрагивающих некоторые требования и механизмы, рассматриваемые в настоящей Рекомендации. Модель угроз безопасности и другие основные материалы рассмотрены в соответствии со следующими Рекомендациями МСЭ-Т:

– [b-ITU-T X.800] определяет общие архитектурные объекты, связанные с обеспечением безопасности, которые могут быть соответствующим образом применены в условиях, когда требуется защитить связь между открытыми системами;
– [b-ITU-T X.805] определяет архитектуру безопасности для обеспечения сквозной безопасности сети.

[b-ITU-T X.800] и [b-ITU-T X.805] определяют следующие угрозы для безопасности сетей:

– уничтожение информации и/или других ресурсов;
– искажение или изменение информации;
– кражу, удаление или потерю информации и/или других ресурсов;
– раскрытие информации;
– прерывание услуг.

В настоящей Рекомендации определяются следующие угрозы, специфичные для мер противодействия кражам мобильных телефонов:

– несанкционированный запрос на удаление данных, находящихся в заблокированном мобильном телефоне;
– несанкционированный запрос блокирования мобильного телефона;
– несанкционированное раскрытие конфиденциальных данных, хранящихся в мобильном телефоне;
– потеря данных пользователя, хранящихся в мобильном телефоне;
– несанкционированный доступ к функциям заблокированного устройства и/или несанкционированное их изменение или к хранящимся в нем данным;
– несанкционированное раскрытие пользовательских данных и программного обеспечения, передаваемых между устройством и оператором сети, и/или средство блокирования для меры противодействия кражам.

Риски заключаются в следующем:

– хакеры могут найти способ имитировать команды блокирования и заблокировать мобильное устройство;
– могут быть раскрыты личные данные, хранящиеся на сервере резервирования или передаваемые между мобильным устройством и сервером резервирования.

7.2 Ключевые функции обеспечения безопасности для мер противодействия кражам мобильных телефонов

Функции блокирования мобильного устройства должны осуществляться только с авторизованного сервера или средства блокирования, поддерживающего функцию блокирования. Для выполнения этого требования необходимы следующие пять функций:

1) наличие безопасного соединения связи между устройством и сервером;
2) аутентификация устройства сервером;
3) аутентификация сервера устройством и получение сервером разрешения на выполнение этой функции;
4) отслеживание местоположения украденного мобильного устройства;
5) безопасное копирование/удаление данных из заблокированного мобильного телефона.

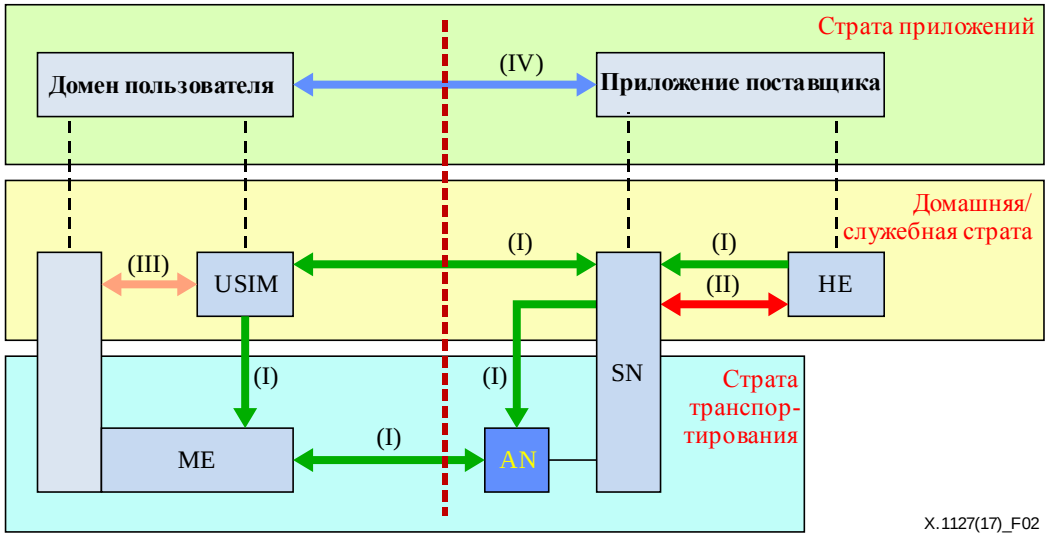
Владельцам устройств должен предоставляться механизм управления информацией, позволяющей установить личность (PII), с их персонального веб-сайта. Владельцу мобильного устройства может предоставляться приложение, установленное на этом устройстве. Приложение для противокражной защиты может предоставлять владельцам устройств возможность выбора защищаемых данных, включая PII, и предусматривать автоматическое копирование данных, включая PII, в облачное решение резервного копирования. Процедура такого управления состоит из следующих трех шагов:

1) установка приложений на мобильное устройство;
2) регистрация на веб-сайте поставщика услуг подвижной связи или производителя устройства;
3) управление (то есть удаление, загрузка, передача) PII, хранящейся на сервере резервирования, через персональный веб-сайт.

7.3 Функциональная архитектура для мер противодействия кражам мобильных устройств

Функциональная архитектура для мер противодействия кражам мобильных устройств основана на архитектуре безопасности, описанной в [b-3GPP TS 33.102]. На рисунке 2 представлена архитектура безопасности, состоящая из пяти групп обеспечения безопасности:

1) безопасность сетевого доступа (I): набор функций безопасности, обеспечивающих пользователям защищенный доступ к услугам 3G и, в частности, защиту от атак по каналам (радио)доступа;
2) безопасность сетевого домена (II): набор функций безопасности, которые позволяют сетевым узлам в домене поставщика безопасно обмениваться сигнальными данными и обеспечивают защиту от атак на сеть проводной связи;
3) безопасность домена пользователя (III): набор функций безопасности, обеспечивающих защищенный доступ к станциям подвижной связи;
4) безопасность домена приложения (IV): набор функций безопасности, которые позволяют приложениям в домене пользователя и домене поставщика безопасно обмениваться сообщениями;
5) видимость и конфигурируемость средств безопасности (V): набор функций, позволяющий пользователю получать информацию о том, работает ли функция безопасности и зависит ли от нее использование и предоставление услуг.



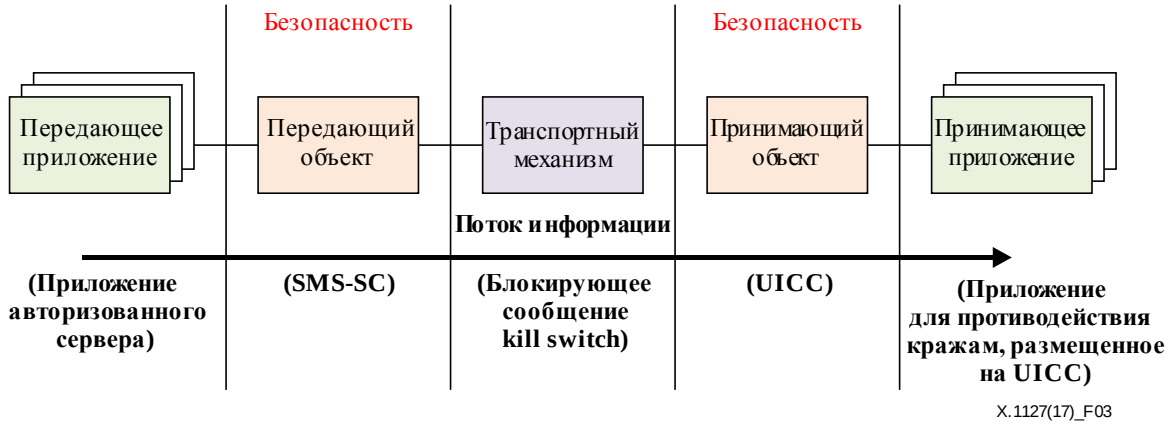
ПРИМЕЧАНИЕ. – Рисунок 2 взят из [b-3GPP TS 33.102].

Рисунок 2 − Архитектура безопасности

Приложение для противокражной защиты в мобильном устройстве является частью набора приложений, размещенных в домене пользователя, а функция противодействия кражам у поставщика услуг – частью набора приложений, размещенных в приложении поставщика.

Эталонная модель безопасности для мер противодействия кражам основана на модели, описанной в [b-3GPP TS 22.048]. Передающее приложение представляет собой объект, генерирующий передаваемое сообщение приложения, а передающий объект – это объект, от которого исходит защищенный пакет (например, центр передачи коротких сообщений (SMS-SC), универсальная карта с интегральной схемой (UICC), пункт ввода неструктурированных данных дополнительных услуг (USSD) или выделенный сервер инструментария универсальных (U) модулей идентификации абонента (SIM)) и который задействует механизмы безопасности. Передающий объект генерирует защищенные пакеты для передачи. Защищенные пакеты передаются через безопасный туннель транспортного уровня или уровня приложения.

Принимающее приложение представляет собой объект, которому предназначено сообщение приложения, а принимающий объект – это объект, получающий защищенный пакет (например, SMS-SC, UICC, пункт ввода USSD или выделенный инструментарий (U)SIM).



ПРИМЕЧАНИЕ. – Рисунок 2 взят из [b-3GPP TS 22.048].

Рисунок 3 − Эталонная модель безопасности

Архитектура безопасности, представленная в настоящей Рекомендации, основана на эталонной модели, показанной на рисунке 1, архитектуре безопасности, показанной на рисунке 2, и эталонной модели безопасности, показанной на рисунке 3.

7.4 Механизмы противодействия кражам мобильных телефонов

7.4.1 Механизмы безопасной связи

Утерянное или украденное устройство должно выступать в качестве сервера аутентификации для клиента безопасного туннеля.

Канал связи между клиентом и сервером должен удовлетворять следующим шести требованиям безопасности.

1) Конфиденциальность. Безопасный туннель должен гарантировать невозможность чтения данных неавторизованными объектами. Это обеспечивается шифрованием данных с использованием криптографического алгоритма и секретного ключа – значения, известного только двум объектам, осуществляющим обмен данными. Данные могут быть расшифрованы только объектом, владеющим секретным ключом.

2) Целостность. Безопасный туннель должен определять, изменены ли данные (намеренно или непреднамеренно) при передаче. Целостность данных обеспечивается путем генерирования значения кода аутентификации сообщения (MAC), который представляет собой криптографическую контрольную сумму данных с ключом. Если данные изменены и код MAC рассчитывается вновь, то его старое и новое значения будут различаться.

3) Взаимная аутентификация. Каждый конечный пункт подтверждает идентичность другого конечного пункта, с которым он желает установить связь, гарантируя тем самым передачу сетевого трафика и данных из ожидаемого узла. Аутентификация безопасного туннеля обычно выполняется в одностороннем порядке как аутентификация сервера клиентом; однако для безопасного туннеля требуется аутентификация обоих конечных пунктов.

4) Защита от повторной передачи. Одни и те же данные не должны передаваться несколько раз и не должны доставляться беспорядочно. В источнике сообщения может использоваться порядковый номер или счетчик. Источник или сообщение присваивает своим пакетам порядковые номера, начиная с 0 и добавляя единицу каждый раз при отправке нового сообщения.

5) Защита от анализа трафика. Лицо, осуществляющее контроль за сетевым трафиком, не должно определять содержание такого трафика или объем передаваемой информации. Безопасный туннель может также скрывать, какие именно стороны обмениваются данными, в то время как SSL оставляет эту информацию открытой. В зависимости от реализации также может быть защищена информация о частоте передачи. Тем не менее количество пересылаемых пакетов может подсчитываться.

6) Управление доступом. Конечные пункты безопасного туннеля должны осуществлять фильтрацию, чтобы обеспечить возможность доступа к определенным сетевым ресурсам только для авторизованных пользователей. Конечные пункты безопасного туннеля также могут разрешать или блокировать определенные типы сетевого трафика, например разрешать доступ к веб-серверам, но запрещать совместное использование файлов.

В целях удовлетворения вышеуказанных требований для обеспечения связи между мобильным устройством и авторизованным сервером рекомендуется использовать TLS (безопасность транспортного уровня). TLS – это протокол, обеспечивающий безопасный туннель связи в сетях. Он позволяет приложениям клиент/сервер взаимодействовать таким образом, чтобы предотвратить перехват, подделку или подлог сообщений. TLS расположен поверх надежных транспортных протоколов (например, протокола управления передачей (TCP)) и используется для инкапсуляции различных протоколов более высокого уровня (например, протокола передачи гипертекста (HTTP)).

Процесс TLS состоит из трех основных этапов:

1) согласование одноранговыми объектами поддерживаемого алгоритма;

2) обмен ключами и аутентификация;

3) симметричное шифрование и аутентификация сообщений.

Подробный профиль TLS приведен в Дополнении V.

В настоящей Рекомендации также предлагается использовать защищенный канал связи на основе протокола OMA (Открытый альянс подвижной связи).

7.4.2 Механизмы взаимной аутентификации

Аутентификация служит для подтверждения идентичности осуществляющих связь объектов. Существует три типа факторов аутентификации:

1) фактор знания ("нечто известное только пользователю"), например пароли;

2) фактор владения ("нечто имеющееся только у пользователя"), например банковские карты (для получения денег в банкомате);

3) фактор свойства ("нечто присущее только пользователю"), например биометрические данные.

В [b-ITU-T X.1158] описаны методы аутентификации трех типов:

1) однофакторная аутентификация (SFA) – это традиционный метод, когда для предоставления пользователю доступа требуется только имя пользователя и пароль;

2) двухфакторная аутентификация (2FA) основана на использовании комбинации двух разных факторов аутентификации. Этими факторами могут быть "нечто известное пользователю", "нечто имеющееся у пользователя" или "нечто присущее пользователю". Хорошим примером из повседневной жизни является снятие денежных средств через банкомат, которое возможно только при предъявлении банковской карты (нечто имеющееся у пользователя) в сочетании с введением персонального идентификационного номера (ПИН-код), то есть "нечто известное пользователю";

3) трехфакторная аутентификация (TFA) основана на использовании комбинации трех различных независимых факторов: "нечто известное пользователю" (пароль), "нечто имеющееся у пользователя" (маркер безопасности) и "нечто присущее пользователю" (биометрическая верификация).

Многофакторная аутентификация основана на использовании комбинации двух или более независимых факторов. Двух- и трехфакторная аутентификация – частные случаи многофакторной аутентификации.

7.4.3 Механизмы безопасного удаления данных

Очистка – это процесс, который делает доступ к целевым данным на носителе невозможным при заданном уровне прилагаемых усилий [b-NIST SP 800-88]. В [b-NIST SP 800-88] определены следующие три категории очистки:

1) операция Clear: применяет логические методы для очистки данных во всех выделенных пользователю областях памяти в целях защиты от простых неинвазивных методов восстановления данных; обычно применяется посредством стандартных команд чтения и записи на запоминающее устройство, например путем перезаписи данных с новым значением или выбора пункта меню для сброса настроек на устройстве до заводских (если перезапись не поддерживается);

2) операция Purge: применяет физические или логические методы, которые делают невозможным восстановление целевых данных с использованием современных лабораторных методов;

3) операция Destroy: делает невозможным восстановление целевых данных с использованием современных лабораторных методов и исключает возможность дальнейшего использования носителя для хранения данных.

Операция Clear позволяет осуществить перезапись данных на носителе путем использования одобренного в организации программного обеспечения и провести проверку перезаписанных данных. Шаблон Clear должен содержать по крайней мере один цикл записи данных с фиксированным значением, таким как все нули. При необходимости можно также использовать несколько циклов записи или более сложные значения.

8 Функциональные требования безопасности

8.1 Обзор

– Функциональная архитектура должна быть построена на основе структуры EAA, описанной в [ITU-T X.1254];

– функциональная архитектура должна обеспечивать безопасный туннель (например, TLS, описанный в [b-IETF RFC 6460], или защищенный канал связи на основе протокола OMA) для связи между компонентами;

– функциональная архитектура должна обеспечивать безопасное управление ключами для поддержки безопасных туннелей (например, на основе инфраструктуры открытых ключей (PKI), описанной в [b-ITU-T X.509]);

– функциональная архитектура должна поддерживать по меньшей мере механизм аутентификации объектов для LoA 2, описанный в [ITU-T X.1254];

– функциональная архитектура должна поддерживать по меньшей мере механизм записи объекта для LoA 2, описанный в [ITU-T X.1254];

– функциональная архитектура должна поддерживать по меньшей мере механизм управления использованием регистрационных данных объекта для LoA 2, описанный в [ITU-T X.1254];

– функциональная архитектура должна поддерживать аутентификацию передаваемых сообщений;

– функциональная архитектура должна поддерживать защиту от атак повторного воспроизведения передаваемых сообщений;

– функциональная архитектура должна поддерживать возможность резервного копирования данных устройства на защищенный сетевой сервер;

– функциональная архитектура должна обеспечивать надежную авторизацию (управление доступом);

– функциональная архитектура должна поддерживать механизмы безопасности, описанные в [b-3GPP TS 22.048];

– функциональная архитектура должна обеспечивать управление определением идентичности владельца мобильного устройства, авторизованного сервера и украденных мобильных устройств.

8.2 Функциональные требования безопасности к владельцу мобильного устройства

– Владелец мобильного устройства должен пройти аутентификацию на авторизованном сервере по меньшей мере на основе 2FA (например, ID/PW плюс одноразовый пароль (OTP), описанный в [ITU-T X.1254]);

– владелец мобильного устройства должен пройти идентификацию с использованием как минимум процедуры записи объекта для LoA 2, описанной в [ITU-T X.1254];

– функциональная архитектура владельца устройства должна аутентифицировать авторизованный сервер с использованием по меньшей мере механизма аутентификации LoA 2, который описан в [ITU-T X.1254];

– функциональная архитектура владельца устройства должна поддерживать безопасный туннель (например, TLS, описанный в [b-IETF RFC 6460], или защищенный канал связи на основе протокола OMA) для обмена сообщениями с авторизованным сервером.

8.3 Функциональные требования безопасности к авторизованному серверу

– Функциональная архитектура авторизованного сервера должна аутентифицировать владельца устройства с использованием по меньшей мере механизма 2FA (например, аутентификаций LoA 3, описанных в [ITU-T X.1254]);

– функциональная архитектура авторизованного сервера должна аутентифицироваться украденным мобильным устройством с использованием по меньшей мере механизма 2FA (например, аутентификаций LoA 3, описанных в [ITU-T X.1254]);

– функциональная архитектура авторизованного сервера должна поддерживать безопасный туннель (например, TLS, описанный в [b-IETF RFC 6460], или защищенный канал связи на основе протокола OMA) для обмена сообщениями с владельцем мобильного устройства;

– функциональная архитектура авторизованного сервера должна поддерживать безопасный туннель для обмена сообщениями с украденным мобильным устройством.

8.4 Функциональные требования безопасности к украденному мобильному устройству

– Функциональная архитектура украденного мобильного устройства должна поддерживать безопасный туннель (например, TLS, описанный в [b-IETF RFC 6460], или защищенный канал связи на основе протокола OMA) для обмена сообщениями с авторизованным сервером;

– функциональная архитектура украденного мобильного устройства должна аутентифицироваться авторизованным сервером с использованием по меньшей мере механизма 2FA (например, аутентификаций LoA 3, описанных в [ITU-T X.1254]);

– функциональная архитектура украденного мобильного устройства должна аутентифицировать авторизованный сервер с использованием по меньшей мере механизма 2FA (например, аутентификаций LoA 3, описанных в [ITU-T X.1254]);

– функциональная архитектура украденного мобильного устройства должна вызывать функцию резервного копирования всех принадлежащих его владельцу данных, хранящихся в устройстве, на безопасный сетевой сервер;

– функциональная архитектура украденного мобильного устройства должна реализовывать механизмы управления доступом для запуска команд, полученных от авторизованного сервера;

– функциональная архитектура украденного мобильного устройства должна защищать данные или функции от доступа и использования неавторизованным объектом;

– функциональная архитектура украденного мобильного устройства при получении команды на удаление данных, хранящихся в мобильном устройстве, от авторизованного сервера должна выполнить операцию Clear для безопасного удаления данных, описанную в пункте 7.4.3.

8.5 Функциональные требования безопасности к серверу резервирования

– Функциональная архитектура сервера резервирования должна поддерживать безопасный туннель для обмена сообщениями с мобильным устройством;

– функциональная архитектура сервера резервирования должна аутентифицировать мобильное устройство с использованием надежного механизма аутентификации, который, при необходимости, выполняет резервное копирование данных устройства;

– функциональная архитектура сервера резервирования должна аутентифицироваться мобильным устройством с использованием надежного механизма аутентификации;

– функциональная архитектура сервера резервирования должна поддерживать возможность резервного копирования соответствующих данных мобильного устройства;

– функциональная архитектура сервера резервирования должна предоставлять мобильному устройству достаточные ресурсы (то есть емкость памяти).

Дополнение I

Общие требования в отношении мер противодействия кражам

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

[b-GSMA] содержит общие требования к информации, относящейся к мерам противодействия кражам. Эти требования описаны в настоящем Дополнении.

I.1 Владелец устройства

– Чтобы подтвердить, что устройство было безвозвратно утеряно или украдено (например, когда координаты глобальной системы определения местоположения (GPS) указывают на нахождение устройства в неизвестном владельцу месте), владелец должен инициировать процедуру блокирования после выполнения следующих действий:
  - подача устройству команды на издание громкого звукового сигнала в течение длительного периода времени (от 30 секунд до 3 минут), чтобы владелец мог найти устройство, в предположении, что оно находится в пределах слышимости;
  - отображение на экране блокировки/главном экране устройства сообщения с просьбой вернуть устройство;
  - установление места нахождения устройства с использованием GPS (или любой другой технологии определения местоположения, если эта функция поддерживается устройством) и отображение его местоположения на карте;
– чтобы отключить функцию блокирования устройства, владелец должен запретить ее явно, а по умолчанию она должна быть разрешена;
– при первоначальном запуске и настройке мобильного устройства рекомендуется демонстрировать владельцу краткую инструкцию по безопасному поведению при использовании и хранении нового устройства. Перед началом работы должно требоваться прочтение инструкции;
– рекомендуется предоставить владельцу устройства возможность доступа к функции блокирования устройства и ее вызова посредством самообслуживания без необходимости привлечения оператора сети;
– рекомендуется не предоставлять владельцу устройства возможности разблокировать устройство, если оно было заблокировано оператором;
– владелец должен иметь возможность вызывать функцию резервного копирования всех принадлежащих ему данных, хранящихся в устройстве (личные данные), на безопасный сетевой сервер;
– владелец должен иметь возможность дистанционно сделать все данные устройства недоступными;
– владелец должен иметь возможность дистанционно удалить из устройства данные пользователя (например, фотографии, видео, телефонную книгу, электронные письма и т. д.). Если данные пользователя надежно зашифрованы, достаточно стереть с устройства ключ шифрования;
– если утерянное или украденное устройство зарегистрировано в гостевой сети (роуминг), владелец может уведомляться о любых дополнительных расходах при попытке вызвать функции резервного копирования данных, блокирования или восстановления работы устройства;
– возможность несанкционированного доступа к функциям отключенного устройства или записанным в нем данным должна быть исключена;
– когда устройство не находится в распоряжении владельца, ему должна быть доступна функция отображения специального сообщения на экране блокировки/главном экране устройства.

I.2 Сервер

– Оператор сети должен аутентифицировать запрос блокирования устройства от владельца устройства.

– Запрос владельца устройства на его блокирование должен быть аутентифицирован и может относиться только к управлению устройством, зарегистрированным на имя этого владельца.

– Информация о местоположении и доступ к серверам, поддерживающим функцию блокирования, должны быть защищены.

– Рекомендуется разрешать доступ к функциям блокирования и их включение только уполномоченному персоналу, обладающему достаточной подготовкой.

– Сервер должен создавать и хранить журналы всех поступивших запросов блокирования.

– При возобновлении обслуживания устройства, восстановленного после блокирования, необходимо вернуть в него все сохраненные за счет резервного копирования данные владельца и приложения.

– Данные владельца, подвергнутые резервному копированию, должны храниться безопасно, с гарантией конфиденциальности и целостности этих данных.

– Как только владелец запросил блокирование своего устройства, он может ожидать, что команда будет выполнена менее чем за 15 минут, если устройство удастся успешно аутентифицировать,

– Восстановление заводских настроек не может использоваться для обхода мер противодействия кражам.

I.3 Мобильное устройство

– Прежде чем переходить к следующим шагам по блокированию устройства, соответствующий запрос должен быть проверен на аутентичность;

– механизмом блокирования мобильного устройства должен управлять авторизованный сервер, поддерживающий функцию блокирования. Для выполнения этого требования необходимо:

  • наличие безопасного соединения между устройством и сервером;

  • аутентификация устройства сервером;

  • аутентификация сервера устройством и получение сервером разрешения на выполнение этой функции;

– при первоначальном запуске и настройке требуется, чтобы мобильное устройство явно инструктировало владельца в процессе установки функций противокражной защиты и любых других соответствующих функций безопасности, таких как механизмы управления доступом к устройству;

– устройство должно обеспечивать возможность восстановления его работы законным владельцем после того, как оно было заблокировано. Возможность восстановления кем-то, кто не является законным владельцем устройства, должна быть исключена;

– рекомендуется, чтобы функция блокирования устройства работала, когда устройство не подключено к сухопутной сети подвижной связи общего пользования, но подключено к интернету;

– если утерянное или украденное устройство зарегистрировано в гостевой сети (роуминг), все функции резервного копирования данных, блокирования и восстановления работы устройства должны успешно выполняться.

I.4 Производство устройств

– Изготовителям устройств рекомендуется продолжать внедрение и разработку мер сдерживания и предотвращения несанкционированного приведения потерянных или украденных устройств в состояние, когда они могут использоваться кем-либо, кроме своего владельца.

Дополнение II

Дополнительные требования безопасности в отношении мер противодействия кражам

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Требования к серверу резервирования

– Механизмом резервного копирования должен управлять сервер резервирования, поддерживающий хранение PII из украденных/утерянных мобильных устройств. Для выполнения этого требования необходимо:

- наличие безопасного соединения между устройством и сервером резервирования;
- аутентификация мобильного устройства сервером резервирования;
- аутентификация сервера резервирования устройством.

Дополнение III

Угрозы, специфичные для мер противодействия кражам

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

III.1 Угрозы, обусловливаемые взаимодействием владельца мобильного устройства и авторизованного сервера

– Маскирование под законного владельца устройства. Злоумышленник направляет на авторизованный сервер злонамеренную команду блокирования, выдавая себя за владельца устройства. Такая атака может привести к нежелательному блокированию мобильных устройств.

– Подлог/перехват/повторная передача сообщений. В авторизованный сервер передается подложная команда блокирования; злоумышленник, способный перехватить сообщение, раскрывает содержание команды либо создается интенсивный трафик, приводящий к распределенным атакам типа "отказ в обслуживании" (DDoS) на авторизованный сервер.

– Подлог авторизованного сервера. Подложный авторизованный сервер позволяет раскрыть регистрационные (учетные) данные для аутентификации законного владельца устройства либо перехватить его команду блокирования устройства. Такая атака может привести к нежелательному блокированию мобильных устройств.

III.2 Угрозы, обусловливаемые взаимодействием авторизованного сервера и средства блокирования в целях противокражной защиты

– Подложный сервер аутентификации. В украденное мобильное устройство поступает злонамеренная команда блокирования.

– Подлог/перехват/повторная передача сообщений. Средству блокирования в целях противокражной защиты передается подложная команда блокирования; злоумышленник, способный перехватить сообщение, раскрывает содержание команды либо создается интенсивный трафик, приводящий к DDoS-атакам на средство блокирования.

– Подложное средство блокирования. Подложное средство блокирования позволяет раскрыть регистрационные данные для аутентификации на легитимном авторизированном сервере или перехватить команду владельца устройства блокирования устройства.

III.3 Угрозы, обусловливаемые взаимодействием средства блокирования в целях противокражной защиты и сервера резервирования

– Подложное средство блокирования в целях противокражной защиты. Подложное средство блокирования раскрывает содержание сообщения, переданного на сервер резервирования.

– Подлог/перехват/повторная передача сообщений. Злоумышленник, способный перехватить сообщение, подменяет и раскрывает содержание резервной копии.

– Подложный сервер резервирования. Подложный сервер резервирования раскрывает содержание резервной копии.

Дополнение IV

Сценарий мер противодействия кражам

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

IV.1 Типы функций блокирования мобильного устройства

Существует два типа функции блокирования:

1) функция "жесткого" блокирования, которая делает украденное мобильное устройство непригодным для использования;

2) функция "мягкого" блокирования, которая делает мобильное устройство непригодным для использования неавторизованным пользователем.

IV.2 Восстановление украденного/утерянного мобильного устройства

Функции противокражной защиты требуют активного участия владельца мобильного устройства. При покупке владельцем нового мобильного устройства и контракта сотового оператора устройство должно быть настроено, чтобы включить функции противокражной защиты.

IV.3 Сценарий блокирования украденного/утерянного мобильного устройства

Если мобильный телефон украден или утерян, владелец связывается со своим поставщиком услуг сотовой связи или использует веб-сайт этого поставщика, выполняющий функции авторизованного сервера, который передает на мобильное устройство команду "заблокировать устройство". Эта команда блокирует мобильное устройство, а также – по желанию владельца устройства – может стереть некоторые хранящиеся в нем личные данные или переписать их на сервер резервирования.

Команда блокирования устройства делает устройство неработоспособным в сети любого поставщика коммерческих услуг подвижной связи или услуг передачи мобильных данных во всем мире, даже если устройство выключено или из него удален носитель данных.

Единственный способ восстановить заблокированное устройство – ввести пароль, предоставленный его владельцем.

Дополнение V

TLS-профиль для мер противодействия кражам

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В данном Дополнении приведен минимальный TLS-профиль для мер противодействия кражам. Типичный пример TLS-профиля представлен в [b-IETF RFC 6460] и [b-ISO/IEC 20648].

V.1 Требования к протоколу TLS

– Для реализации протокола TLS рекомендуется использовать систему противокражной защиты, действующую в качестве сервера; однако ее использование клиентами не обязательно. Должна быть реализована версия TLS 1.2 (указанная в [b-IETF RFC 5246]) или более поздняя версия.

V.2 Совместимые наборы параметров шифрования TLS

– В системе противокражной защиты не следует использовать MD5 или SHA-1 в качестве хешированного кода аутентификации сообщений по умолчанию (HMAC);

– в системе противокражной защиты не следует использовать RC4 в качестве криптографического алгоритма по умолчанию;

ПРИМЕЧАНИЕ. – [b-IEFT RFC 7465] запрещает использование RC4.

– система противокражной защиты должна поддерживать выбор и использование пар алгоритмов "подпись/хеш" с алгоритмами подписи, поддерживаемыми в версии TLS 1.2, и SHA-256 или более сильными хеш-алгоритмами;

– в системе противокражной защиты должны использоваться наборы параметров шифрования с уровнем надежности защиты не менее 112 бит. Кроме того, должны поддерживаться следующие наборы параметров шифрования:

  • TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}.

V.3 Цифровые сертификаты

Система противокражной защиты должна поддерживать сертификаты открытого ключа [b-ITU-T X.509] версии 3, соответствующие профилю сертификатов и расширений сертификатов, определенному в разделе 4 [b-IETF RFC 5280]:

– TLS-сервер в системе противокражной защиты должен поддерживать сертификаты сервера;

– рекомендуется, чтобы в системе противокражной защиты TLS-клиент поддерживал сертификаты клиента;

– система противокражной защиты должна поддерживать ключи сертификатов сервера RSA/DSA МСЭ-T X.509 размером 2048 битов и более;

– система противокражной защиты должна поддерживать форматы сертификатов [b-ITU-T X.509] в кодировке отличительных правил кодирования (DER), [b-ITU-T X.509] в кодировке Base64 и PKCS#12 [b-IETF RFC 7292];

– система противокражной защиты должна поддерживать проверку сертификата, как описано в разделе 6 документа [IETF RFC 5280], в котором представлен цифровой сертификат. Кроме того, чтобы определить, не был ли сертификат аннулирован, используется один из следующих подходов.

  • Вариант 1: Использование списков аннулированных сертификатов (CRL): поддерживаемые CRL форматов [b-ITU-T X.509]в кодировке DER или [b-ITU-T X.509]в кодировке Base64 и действительные CRL, хранимые локально (распределение не входит в сферу применения настоящего стандарта) или извлекаемые из внешнего источника (например, точка распределения CRL (CRLDP)).

- Вариант 2: Использование протокола статуса сертификата, такого как онлайновый протокол статуса сертификата (OCSP), одним из следующих способов: непосредственное использование OCSP, как указано в [b-IETF RFC 6960], или косвенное использование OCSP посредством расширения запроса статуса сертификата протокола TLS, как указано в разделе 8 [b-IETF RFC 6066].

Дополнение VI

Обзор протокола управления устройствами OMA

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В данном Дополнении представлен обзор протокола управления устройствами (DM), определенного OMA [b-OMA-DM].

VI.1 Спецификация управления устройствами OMA

Спецификация DM OMA предназначена для управления мобильными устройствами, такими как мобильные телефоны, персональные цифровые ассистенты и планшетные компьютеры. Управление устройствами призвано поддерживать следующие виды деятельности:

– инициализация: выбор конфигурации устройства (в том числе при использовании в первый раз), функции включения и выключения;

– настройка устройства: внесение изменений в настройки и параметры устройства;

– обновление программного обеспечения: загрузка нового программного обеспечения и/или исправлений, включая приложения и системное программное обеспечение;

– устранение неисправностей: сообщения об ошибках, запросы состояния устройства.

Все вышеперечисленные функции поддерживаются спецификацией DM OMA, и в устройстве могут быть факультативно реализованы все эти функции или часть из них. Поскольку спецификация DM OMA предназначена для мобильных устройств, она разработана с учетом следующих факторов:

– компактные устройства, в которых емкость оперативной и долгосрочной памяти может быть ограничена;

– ограниченная пропускная способность линии связи, как, например, в случае беспроводной связи;

– жесткий контроль безопасности, поскольку устройства уязвимы для программных атак; в спецификации рассматриваются вопросы аутентификации и решения проблем.

Библиография

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*

[b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.*

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

[b-ITU-T X.1250] Рекомендация МСЭ-Т X.1250 (2009 г.), *Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности.*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*

[b-ITU-T X-Sup.19] Рекомендации МСЭ-Т серии X – Добавление 19 (2013 г.), *Добавление по аспектам безопасности смартфонов.*

[b-ISO/IEC 20648] ISO/IEC 20648:2016, *Information technology – TLS specification for storage systems.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-3GPP TS 22.048] 3GPP TS 22.048 (2003), *Security mechanisms for the (U)SIM Application Toolkit*, June 2003.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2009), *3G Security; Security architecture (Release 9)*, December 2009.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2.*

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

[b-IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions.*

[b-IETF RFC 6460] IETF RFC 6460 (2012), *Suite B Profile for Transport Layer Security (TLS).*

[b-IETF RFC 6960] IETF RFC 6960 (2013), *ITU-T X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[b-IETF RFC 7292] IETF RFC 7292 (2015), *PKCS #12 Personal Information Exchange Syntax v1.1.*

[b-IETF RFC 7465] IETF RFC 7465 (2015), *Prohibiting RC4 Cipher Suites.*

[b-GSMA] GSMA, *SG.24 Anti-Theft Device Feature Requirements v3.0*, 17 May 2016.

[b-OMA-DM] Open Mobile Alliance, *OMA Device Management V1.2*, April 2013.

[b-NIST SP 800-88] NIST, *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization*, December 2014.

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
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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.