Международна работна група
по защита на личните данни
в телекомуникациите

675.52.10

Работен документ: Актуализация на въпросите за личната неприкосновеност и сигурността при интернет телефонията и свързаните с нея комуникационни технологии

59-та среща, 24-25 април 2016, Осло (Норвегия)

Въведение

През септември 2006 Групата публикува работен документ относно приложенията[1], използващи интернет телефония, с цел да изпревари събитията и да идентифицира възможни бъдещи предизвикателства за личната неприкосновеност и сигурността. Документът обрисува ситуацията така както Групата я виждаше по това време: той съдържаше описание на нововъзникващите услуги, възможните бъдещи рискове за неприкосновеността и сигурността, както и набор от препоръки към производителите на устройства, разработчиците на софтуер и доставчиците на интернет телефония.

През следващите 10 години интернет телефонията доби все по-широка употреба от бизнеса и потребителите. Нещо повече, тя бе интегрирана и внедрена в още редица комуникационни технологии, като например тези за комуникация в реално време (чрез текст, картина или аудио съобщения). В някои региони дори вече текат дебати дали аналоговата телефонна мрежа следва да бъде извадена от употреба, тъй като много хора вече я считат за технология от миналото.

Препоръките в работния документ се отнасят до всички мултимедийни услуги, включително чатовете в реално време и видео услугите[2]. Този документ освен това не прави никакво разграничение между интернет телефонията предлагана от телекомуникационен оператор и OTT доставчик (компания предлагаща телевизионно или филмово съдържание през интернет). Дори технологията, предлагана от различните компании, да се различава, рисковете за неприкосновеността и защитата на личните данни остават сходни, за това препоръките се отнасят за всички.

В допълнение към стандартизираните решения съществуват множество авторски продукти и услуги, които осигуряват различна степен на сигурност и защита на личните данни. За съжаление ползвателите, които не са тясноспециализирани в областта, често остават

[1] Международната работна група по защита на личните данни в телекомуникациите: „Работен документ относно неприкосновеността и сигурността при използването на интернет телефония“, приет на 40 - тата среща на групата, 5-6 септември, Берлин; http://www.datenschutzberlin.de/attachments/102/WP_VoIP_en.pdf

[2] Термините „глас и видео“ и „мултимедия“ се припокриват, тъй като съдържанието на препоръката се отнася до най-всеобхватната концепция на мултимедийната комуникация, но поради исторически причини и по-лесно възприемане от страна на четящите по-често в текста ще срещнете термина „глас“.

неинформирани за предлаганата защита или не получават такава защита, при която е спазен принципът на неприкосновеност по подразбиране.

С настоящия работен документ Групата допълва препоръките от първата публикация, въз основа на преоценка на ситуацията (спрямо 2016 г.). Следните съображения налагат преоценката на темата:

- Разкритията на Едуард Сноудън показват, че правоприлагащите органи и тайните служби по света имат безпрецедентен достъп до разговорите, извършвани чрез интернет телефония и съпътстващите ги трафични данни, с или без съдействието на компаниите, които предлагат услугата. Това глобално следене уронва доверието. както към разработчиците, така и към доставчиците на услугата. Течовете на трафични данни, като IP адреси, DNS искания и сигнализиращи слоеве също така представляват предизвикателства за опазването на поверителността на информацията[3]. Въпреки че тези трафични данни не разкриват съдържанието на комуникацията, те са достатъчни за да компрометират неприкосновеността на индивида.

- Прогресът в стандартизацията на интернет телефонията доведе до узряване на пазара спрямо 2006 г. когато бе публикуван първият документ. Стандартизацията на протоколите за иницииране на сесията (SIP) и на различните разширения бе финализирана и понастоящем има множество продукти, които са достъпни на пазара. Освен това бе започната разработката (вече са достъпни пробни версии) на нов стандартизационен продукт, по-конкретно „Онлайн комуникация в реално време“ (WebRTC)[4], който цели да предложи по-добра интеграция с мрежовите технологии и в частност уеб браузърите. Това поражда нови заплахи за сигурността и неприкосновеността[5].

- Употребата на широколентови клетъчни радио радиотехнологии и Wi-Fi мрежи се е увеличила значително. Потребителите вече могат да използват тези мрежи за провеждането на надеждни разговори чрез интернет телефония. Освен това софтуерът за интернет телефония вече е лесен за ползване и за набавяне, било то чрез фабрично инсталиране на самите устройства или чрез магазините за приложения. В началото на века интернет телефонията бе ползвана предимно от бизнеса и технически грамотните ползватели докато днес тя се ползва на практика от всички.

- Практиките, свързани със сигурността и неприкосновеността варират значително спрямо различните предлагани услуги. За съжаление, тези практики не са обяснени достатъчно добре на ползвателите на услугите.

- Аналоговите телефонни мрежи в миналото бяха традиционно изграждани и управлявани от един единствен оператор, в съдружие с държавата. Ситуацията с интернет телефонията е напълно различна, тъй като средата при нея еволюира в мозайка от няколко съставни части (например мрежови услуги, операционни

[3] R. Barnes, et al., " Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem R. Barnes, et al., " https://tools.ietf.org/html/rfc7624

[4] Real-time Communication Between Browsers, достъпен на http://www.w3.org/TR/webrtc/http://www.w3.org/TR/webrtc/

[5] E. Rescorla, "WebRTC Security Architecture", IETF draft (work in progress), March 2015, на адрес https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-11

системи, приложен софтуер). Често тези „части“ се разработват и управляват от различни организации (например мрежови оператори, софтуерни разработчици, производители на устройства и тн.), като всеки от тях функционира независимо и в повечето случаи без координация с останалите. Това разнообразие осигурява по-големи възможности за избор на ползвателите, но не и по-високо ниво на защита на неприкосновеността и личните данни им данни, тъй като всяка организация се фокусира върху нейната част от веригата.

Технически характеристики

Като идея, интернет телефонията е принципно проста: потребителят въвежда телефонен номер или друг идентификатор (много от тях напомнят на мейл адреси) за да „набере“ друг потребител. Чрез помощна инфраструктура потребителят стартира сигнална комуникация, за да намери устройството на търсената страна. Съобщенията разменени по време на тази процедура се наричат сигнални съобщения.

При интернет услуги, които не поддържат възможност за взаимодействие с други доставчици, всички потребители трябва да имат регистрация при съответния доставчик на услугата. При по-отворените системи намирането на адресата може да е по-усложнено тъй като потребителите могат да имат регистрации при различни доставчици на телефония, а намирането на дадения адресат може да включва и участието на трети доставчик. Трябва да се отбележи, че комуникацията през различни доставчици (или дори чрез публичната телефонна мрежа) може да доведе до загуба на функционалност и отслабване на защитните механизми.

Веднъж след като устройството на търсената страна е било намерено, между участниците могат да се обменят звукови съобщения (наричани гласови пакети). По принцип сигналните съобщения често се прекарват през помощна инфраструктура, докато мултимедийният трафик (например глас и видео) обикновено се предава директно между двете страни. Директната комуникация осигурява по-добра синхронизация. Гласовите пакети могат да бъдат предавани чрез Безопасния протокол за предаване на данни в реално време (SRTP)[6] . Съществуват и други протоколи, които се използват за намаляване на риска от следене или прихващане на съобщенията[7].

На практика, сигналните съобщения предлагат повече функционалности отколкото само идентифицирането на комуникационните устройства, като например уточняване на параметрите и характеристиките на протокола. За някои сценарии, например при видеоконферентни връзки или трансфери на обаждания, процедурата за осъществяване на обаждането може да бъде по-сложна. Нещо повече, за да се осигури сигурност на комуникационните канали чрез SRTP са нужни криптографски ключове и алгоритми. За това бяха разработени протоколи за работа с криптографски ключове, с които могат да се създават ключове за защита на мултимедийния трафик. Всички имат незначително различаващи се характеристики[8].

---

[6] M. Baugher, et al., "The Secure Real-time Transport Protocol (SRTP)", March 2004, RFC 3711, available at https://tools.ietf.org/html/rfc3711

[7] Становището на IAB относно интернет поверителността от ноември 2014, available at https://www.iab.org/2014/11/14/iab-

[8] За анализ на ключовите технологии за обмен и техните характеристики посетете RFC 5479 (https://tools.ietf.org/html/rfc5479) както и RFC 7201 (https://tools.ietf.org/html/rfc7201)

Препоръки[9]

С оглед на гореизложеното Работната група отправя следните препоръки към заинтересованите страни:

Законодатели и регулатори

На законодателите и регулаторите на национално, регионално и дори глобално ниво следва да се припомни, че съществуват пропуски в системите за правна защита на поверителността на комуникациите по отношение на интернет телефонията. Призивът към тях е внимателно и задълбочено да проучат правната ситуация и да направят необходимите промени, с които разпоредбите в националните конституции, регионалните и глобални регулаторни инструменти отнасящи се до поверителността на телекомуникациите, да обхванат и интернет телефонията и останалите мултимедийни комуникационни услуги.

Доставчици, софтуерни разработчици и производители на устройства

Прозрачност

Доставчиците на интернет телефония би следвало да информират клиентите относно характеристиките по отношение на сигурността и неприкосновеността на услугите, които предлагат.

Независимата оценка на въздействието върху неприкосновеността

Разработчиците и производителите следва да извършват оценка на въздействието върху неприкосновеността. Работната група също така насърчава анализа и оценката от независими, авторитетни трети страни. Пример за такава оценка е „Индексът за сигурни съобщения“, разработена от Electronic Frontier Foundation (EFF)[10]. Примери за автоматизирани инструменти са продуктите на Фондация XMPP[11] както и сайтът GSM map[12].

Съображения при проектиране

Разработчиците и производителите следва да предприемат подходящите технически мерки за защита на сигналния, звуковия и видео трафик срещу нерегламентирано проследяване.

Наложително е при проектирането на своите продукти разработчиците да се стремят да използват решения базирани на криптиране тип „от край до край“ както за сигналната така и за останалата комуникация.

Сигналният трафик на интернет телефонията трябва да се удостоверява, а целостта и

[9] Препоръките за интернет телефонията трябва да бъдат възприемани в контекста на тези от първия Работен документ от 2006; cf. http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_en.pdf

[10] Electronic Frontier Foundation (EFF), “Secure Messaging Scorecard”, October 2015, available at https://www.eff.org/secure-messaging-scorecard

[11] XMPP (Extensible Messaging and Presence Protocol) Foundation, “XMPP Security Tests”, October 2015, http://xmpp.net

[12] GSM – *Global System for Mobile* Communications (previously „Groupe Spécial Mobile“). Cf. Karsten Nohl, “GSM Map”, October 2015, available at https://gsmmap.org

поверителността между участващите страни трябва да бъдат защитени. За съжаление, повечето продукти са изградени така, че осигуряването на цялостност „от край до край“ при тях не е възможно, тъй като съобщенията се преобразуват по време на трансфера[13].
9

Предаването на сигнални съобщения по некриптирани мрежи трябва да бъде избягвано. Трябва да се отбележи, че да се разчита единствено на физическата защита не е надеждна техника за сигурност при настоящето ниво на наблюдение в Интернет[14].

Трафичните данни от комуникацията, като например идентификаторите на общуващите страни, комуникационните предпочитания (като език и кодеци), дължината на (криптираните) пакети данни и онлайн статусът, често разкриват изненадващо много информация. За това Работната група препоръчва да се ограничи обемът данни, който преминава през посредници, като например сигналните гейтуей мрежи и да се избягва употребата на перманентни идентификатори, доколкото е възможно.

Работната група силно окуражава доставчиците на интернет телефония да използват такива механизми за управление на криптографски ключове, които не позволяват на посредниците да се сдобият с информацията за създаване на ключове (тъй като тя се предава като нормален текст, вграден в сигналните съобщения) и да употребяват протоколи, които предлагат PFS[15] (Perfect Forward Security). PFS е инструмент за сигурност, който не позволява на зложелателите да дешифрират миналите разговори, в случай че сигурността на дългосрочните ключове е компрометирана. Въпреки съществуващите ограничения в софтуерната архитектура на интернет телефонията, приоритет трябва да бъде поставен върху интегрирането на принципа за сигурност „от край до край“ в гласовата и видео комуникация. Една от възможностите за това е трети страни да издават сертификати, които да бъдат навързани с псевдоними (телефонни номера, потребителски имена, имена на организации) и те да бъдат разкривани на страните в комуникацията[16].

Доставчиците на интернет телефония трябва по подразбиране на ограничават обема на лични данни, които се обработват и съхраняват за осигуряването и разплащането (ако е приложимо) на услугата, освен ако допълнителното обработване или съхранение на данни не се налага поради законово изискване. Трябва да бъде изградена и защита срещу неоторизиран достъп до съхраняваните данни..

Доставчиците на интернет телефония трябва да предлагат поне базови механизми за защита на неприкосновеността, като например възможността за скриване самоличността на обаждащата се страна, поне по начина, по който това се прави при стационарните и мобилни телефонни мрежи. Тъй като тези процедури улесняват някои специфични видове атаки, следва да се обърне внимание на някои скорошно разработени механизми за

---

[13] Тъй като модификацията на сигналните съобщения променя алгоритмите на подписа, както е описано на страница 16 от RFC 7340 (https://tools.ietf.org/html/rfc7340), а повечето софтуери за интернет телефония модифицират сигналните съобщения по време на предаването, броят на участващите точки за връзка трябва да бъде колкото се може по-малък. RFC 7044 предлага решение за защита на съобщенията, като при него те се прекарват през SIP комуникационната мрежа. Това дава възможност да се съхранява информация за комуникацията, която да е достъпна за участниците в (https://tools.ietf.org/html/rfc7044).

[14] В миналото кабелната мрежа, използвана за класическата телефонна комуникация се считаше за безопасна, но това вече не е валидно, тъй като тайните служби по света проникват масово в комуникационната инфраструктура.

[15] PFS е подробно обяснена тук: https://en.wikipedia.org/wiki/Forward_secrecy . Cf also A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, USA, 1996 (see page 496).

[16] J. Peterson, et al., "Secure Telephone Identity Credentials: Certificates", IETF draft (work in progress), March 2016, на страница https://tools.ietf.org/html/draft-ietf-stir-certificates-03

защита[17]. Прикриването на самоличността на обаждащия се понижава ефективността на списъците за контрол на достъпа. Поради директната връзка между двете общуващи страни пък техните IP адреси ще бъдат разкрити по време на комуникацията. За да се предотврати това, употребата на прокси сървъри или анонимизиращи услуги (например Tor[18], TURN[19]) не трябва да бъде забранявана.

Съществуващите отворени стандарти[20],[21], които са преминали оценка и верификация от широк кръг от независими експерти, трябва да бъдат повторно вкарани в употреба. Има няколко стандартизирани решения за защита на гласова комуникация, които са достъпни към настоящия момент. Следва да се отбележи, че процесът по стандартизация в различните организации позволява техническите спецификации да бъдат публикувани без да преминат задълбочена експертна оценка или в най-лошия случай, без какъвто и да било преглед. За това е нужно решението какви технически спецификации да бъдат използвани да отчита и нивото на оценка. Насърчават се също така органите по стандартизация да залагат на повече прозрачност в процеса, чрез който се разработват спецификациите.

Потребителско участие

Доставчиците на интернет телефония следва да позволят на своите потребители сами да избират доставчика на своята виртуална идентичност, в случаите когато е технически възможно да се направи разграничението между доставчик на телефония и доставчик на идентичност.

Доставчиците на интернет телефония следва да създадат възможност за преносимост на данните (там където е подходящо), за да осигурят на своите клиенти удобен достъп до съответните данни, сред които са разрешените списъци и данните за настройките на услугата.

Някои оперативни съображения

Всички участници във веригата за доставка на услугата трябва да реагират бързо на откритите пропуски и нередности в протоколите или използваните хардуер и софтуер. За грешки в софтуера, например в приложенията за смартфони или друг софтуер за сваляне, това изисква инкорпорирането на механизъм за обновяване на софтуеъра.

Доставчиците на интернет телефония трябва да се уверят, че механизмите, защитаващи сигурността и неприкосновеността в техните продукти, са активирани по подразбиране. Тези механизми трябва да се предлагат без разходи, възпрепятстващи ползвателите.

Доставчиците на интернет телефония следва да предлагат възможността за съвкупен достъп до техните услуги, т.е. потребителите да могат да взаимодействат с ползватели на

[17] IETF, “Secure Telephone Identity Revisited (STIR) Working Group”, October 2015, available at http://datatracker.ietf.org/wg/stir/charter/

[18] Повече информация за Tor може да бъде намерена на https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[19] R. Mahy, et al., "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, Apr. 2010, available at https://tools.ietf.org/html/rfc5766

[20] M. Westerlund and C. Perkins, "Options for Securing RTP Sessions", RFC 7201, April 2014, достъпна на адрес https://tools.ietf.org/html/rfc7201

[21] D. Wing, et al., "Requirements and Analysis of Media Security Management Protocols", RFC 5479, April 2009, https://tools.ietf.org/html/rfc5479

други подобни услуги, без да се налага да инсталират няколко различни софтуера за интернет телефония на техните устройства. Най-малкото потребителите следва да бъдат информирани за всякакви изменения в сигурността и неприкосновеността, които са следствие от взаимодействието с друг софтуер за интернет телефония или даналоговата телефонна мрежа, както и за всякаква загуба на функционалност или намаляване на защитата, произтичащи от това взаимодействие.

Целесъобразност

Доставчиците , разработчиците и производителите на хардуер, които обработват трафични данни трябва да спазват принципа на целесъобразност.

Потребители

Потребителите на интернет телефония трябва да са наясно с възможните рискове за сигурността и неприкосновеността на тяхната комуникация. Те следва да се информират относно техническите характеристики на различните предлагани услуги и да базират избора си за предпочитани услуги спрямо тях. Освен това още преди ползването на дадената услуга те трябва да се уверят, че наличните защитни механизми са активирани.

Информация за Международната работна група за защита на личните данни в телекомуникациите (“Берлинска група”)

Международната работна група за защита на личните данни в телекомуникациите (IWGDPT, известна още като “Берлинска група”) включва представители от органите за защита на данните и международни организации от всички краища на света, занимаващи се с въпросите на неприкосновеността на личния живот. Тя е основана през 1983 г. в рамките на Международната конференция на защита на личните данни и неприкосновеността на личния живот по инициатива на берлинския комисар по защита на данните, който оттогава председателства Групата. От 1983 г. до сега Групата е приела многобройни препоръки („Общи позиции“ и „Работни документи“), насочени към подобряване на защитата на личната неприкосновеност в сферата на телекомуникациите. От началото на 90-те години Групата се фокусира по-специално върху защитата на личните данни в Интернет.
Повече информация за работата на групата и приетите от нея документи може да бъде намерена на уебсайта на самата група http://www.berlin-privacy-group.org.