Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.

May 2014

Всеобъемлющий мониторинг является атакой

Pervasive Monitoring Is an Attack

Тезисы

Всеобъемлющий мониторинг является технической атакой, которую следует, по возможности, подавлять уже на этапе разработки протоколов IETF.

Статус документа

Этот документ относится к категории «Обмен опытом» (Best Current Practice).

Документ является результатом работы IETF[1] и представляет согласованное мнение сообщества IETF. Документ был подвергнут открытому обсуждению и одобрен для публикации IESG[2]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе документа, обнаруженных ошибках и способах обратной связи приведена на странице http://www.rfc-editor.org/info/rfc7258.

1. Всеобъемлющий мониторинг — широко распространенная атака на приватность

Всеобъемлющий мониторинг (PM[3]) - широко распространенное (и зачастую скрытное) наблюдение путем сбора протокольных образцов, включая содержимое данных приложений или метаданные протоколов (например, заголовки). Активное или пассивное «прослушивание» (wiretap) и анализ трафика (например, поиск корреляций и синхронизации или измерение размера пакетов) или «взлом» (subverting) криптографических ключей, применяемых для защиты протоколов, также могут быть частью всеобъемлющего мониторинга. PM отличается отсутствием избирательности и очень широким охватом, но не создает новых типов технических опасностей.

С технической точки зрения сообщества IETF PM представляет собой атаку на приватность пользователей и организаций в сети Internet. Сообщество IETF решительно заявляет, что PM является атакой, которую следует по возможности ослаблять уже на уровне разработки протоколов, чтобы сделать мониторинг более дорогостоящим или неосуществимым. Всеобъемлющий мониторинг на пленарной технической сессии конференции IETF в ноябре 2013 года [IETF88Plenary], а также активно обсуждался в почтовых конференциях IETF. Данный документ выражает согласованное мнение сообщества IETF и обосновывает техническую природу PM.

Термин «атака» (attack) употребляется здесь в техническом смысле, который несколько отличается от общепринятого толкования этого слова в английском языке. В общепринятой трактовке атака представляет собой агрессивное действие, предпринимаемое противником для принуждения атакуемой стороны к исполнению воли атакующего. Здесь этот термин служит обозначает вмешательство в процесс коммуникационного взаимодействия без согласия его участников. При атаке может менять содержимое информационного обмена, выполняться запись содержимого или каких-либо характеристик коммуникаций, а также сопоставление с другими коммуникационными событиями, раскрывающее информацию, которую взаимодействующие стороны не были намерены раскрывать. Мониторинг PM может оказывать и другие влияния, нарушающие намерения взаимодействующих сторон. Более полное определение термина «атака» приведено в [RFC4949]. Термин атака используется здесь в единственном числе, хотя на практике PM может представлять собой множество скоординированных атак.

В частности, атака в техническом смысле не включает никаких предположений о намерениях атакующего. Мотивом организации PM может быть нецелевое наблюдение со стороны государства, законные, но ущемляющие приватность других действия коммерческих структур, а также незаконные действия криминальных структур. Используемые для реализации PM методы на зависят от мотивов организатора. Таким образом, мы не может защититься от злоумышленников, позволяя кому-либо выполнять мониторинг, поскольку выполняемые для него действия не зависят от целей мониторинга. Следовательно, мотивы не имеют значения для подавления PM в протоколах IETF.

[1] Internet Engineering Task Force.
[2] Internet Engineering Steering Group.
[3] Pervasive Monitoring.

2. IETF будет бороться с всеобъемлющим мониторингом

Подавление (Mitigation) — технический термин, не предполагающий возможность полного предотвращения или существенно осложнить атаку. Протоколы, препятствующие PM не предотвратят атаку, но смогут существенно ослабить угрозы (см. график на странице 24 RFC 4949, где показана связь между терминами «атака» и «угроза»). Подавление может существенно повысить стоимость атаки и осложнить ее сокрытие или упростить обнаружение.

Стандарты IETF уже включают механизмы для защиты коммуникаций Internet и в [RFC3552] приведены рекомендации по использованию этих механизмов при разработке протоколов. Но эти стандарты в основном не связаны с PM, конфиденциальностью метаданных протоколов, противодействием анализу трафика или минимизацией данных. В любом случае остается некоторый объем связанных с приватностью данных, которые неизбежно раскрываются протоколами. По мере развития технологий методы, которые раньше были доступны только при очень хорошем финансировании, получают более широкое распространение. Следовательно, подавление PM является защитой от широкого класса похожих атак.

Следовательно, настало время пересмотреть стандарты в части безопасности и приватности. IETF будет работать над техническими аспектами подавления PM, как это делается для устранения протокольных уязвимостей. Способы, с помощью которых в протоколах IETF будет подавляться PM, будут меняться со временем, по мере развития технологий подавления и разработки новых методов атак, которые не описаны здесь.

От разработчиков спецификаций IETF требуется способность описать, как они учитывали возможность PM и, если атаки применимы к публикуемой работе, способность предложить соответствующие решения для подавления таких атак. Это не означает необходимости включения в документы IETF нового раздела «Вопросы всеобъемлющего мониторинга». Это означает, что при возникновении вопроса о возможности всеобъемлющего мониторинга, относящегося к публикуемой работе, не него был дан четкий и недвусмысленный ответ.

В частности, архитектурные решения, включая выбор для использования уже имеющихся технологий, могут оказывать существенное влияние на уязвимость протокола для PM. Разработчикам спецификаций IETF, следовательно, требуется принимать во внимание вопросы подавления PM при выборе архитектурных решений. Получение адекватного и своевременного обзора архитектурных решений, включая вопрос о целесообразности мер подавления PM, может иметь важное значение. Последующий пересмотр принятых ранее архитектурных решений обойдется значительно дороже.

Хотя PM признан атакой, могут существовать некоторые формы мониторинга, формально соответствующие определению PM, но не представляющие собой атаки и способные приносить пользу (например, функции сетевого управления для мониторинга пакетов или потоков, а также механизмы предотвращения спама, просматривающие содержимое электронной почты). Некоторые варианты мониторинга могут даже послужить частью процесса подавления PM (например, прозрачность сертификатов [RFC6962] включает мониторинг инфраструктуры PKI[1], позволяющий обнаруживать некоторые методы атак PM). Однако очевидна возможность использования механизмов мониторинга для организации PM, поэтому эти вопросы требуют внимательного рассмотрения в процессе разработки протоколов. Потеря управляемости сетей в результате подавления PM является неприемлемым результатом, но игнорирование PM противоречило бы описанному в этом документе соглашению. Со временем должен быть найден разумный баланс по мере развертывания реальных образцов.

Отметим, что IETF, как разрабатывающая стандарты организация, не контролирует реализацию или развертывание выпущенных спецификаций (хотя среди участников IETF имеется множество разработчиков реализаций) и не стандартизует все уровни стека протоколов. Кроме того, не технические (например, юридические или политические) аспекты подавления всеобъемлющего мониторинга не входят в сферу деятельности IETF. Широкое сообщество Internet должно сделать шаг вперед в решении проблемы PM, если есть желание решить ее полностью.

В качестве заключения отметим, что современные возможности позволяют организовать мониторинг содержимого и метаданных в сети Internet, масштабы которого раньше было просто невозможно представить. Этот всеобъемлющий мониторинг является атакой на приватность Internet. IETF будет стремиться к разработке спецификаций, позволяющих смягчить влияние таких атак.

3. Замечания по процессу

В прошлом связанные с архитектурой заявления такого типа (например, [RFC1984] и [RFC2804]) публиковались от имени IESG[2] и IAB[3]. Однако с момента публикации упомянутых документов IETF и IAB разделили «потоки» своих публикаций, как описано в [RFC4844] и [RFC5741]. Данный документ был инициирован после обсуждения в IESG и IAB, но публикуется, как согласованное мнение IETF для того, чтобы корректно отразить согласованную точку зрения IETF в целом.

4. Вопросы безопасности

Этот документ целиком посвящен приватности. Дополнительную информацию о связях между угрозами безопасности и приватности можно найти в [RFC6973]. Параграф 5.1.1 в [RFC6973] посвящен конкретному рассмотрению наблюдения, как комбинированной угрозы безопасности и приватности.

5. Благодарности

Благодарим участников пленарной технической секции IETF 88 за их отклики. Отдельная благодарность за полезные приложения и комментарии Jari Arkko, Fred Baker, Marc Blanchet, Tim Bray, Scott Brim, Randy Bush, Brian Carpenter, Benoit Claise, Alissa Cooper, Dave Crocker, Spencer Dawkins, Avri Doria, Wesley Eddy, Adrian Farrel, Joseph Lorenzo Hall, Phillip Hallam-Baker, Ted Hardie, Sam Hartmann, Paul Hoffman, Bjoern Hoehrmann, Russ Housley, Joel Jaeggli, Stephen Kent, Eliot Lear, Barry Leiba, Ted Lemon, Subramanian Moonesamy, Erik Nordmark, Pete Resnick, Peter Saint-Andre, Andrew Sullivan, Sean Turner, Nicholas Weaver, Stefan Winter и Lloyd Wood. Спасибо также всем тем, кто считает, что внес свои

[1] Public Key Infrastructure — инфраструктура обмена открытыми ключами.
[2] Internet Engineering Steering Group.
[3] Internet Architecture Board.

предложения в части повышения уровня защиты и сохранения приватности в Internet, а также всем, кто комментировал эти вопросы в разных почтовых конференциях IETF типа ietf@ietf.org и perpass@ietf.org.

6. Литература

[IETF88Plenary] IETF, "IETF 88 Plenary Meeting Materials", November 2013, <http://www.ietf.org/proceedings/88/>.

[RFC1984] IAB, IESG, Carpenter, B., and F. Baker, "IAB and IESG Statement on Cryptographic Technology and the Internet", RFC 1984, August 1996.

[RFC2804] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC4844] Daigle, L. and Internet Architecture Board, "The RFC Series and RFC Editor", RFC 4844, July 2007.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5741] Daigle, L., Kolkman, O., and IAB, "RFC Streams, Headers, and Boilerplates", RFC 5741, December 2009.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, June 2013.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

Адреса авторов

Stephen Farrell

Trinity College Dublin

Dublin 2

Ireland

Phone: +353-1-896-2354

EMail: stephen.farrell@cs.tcd.ie

Hannes Tschofenig

ARM Ltd.

6060 Hall in Tirol

Austria

EMail: Hannes.tschofenig@gmx.net

URI: http://www.tschofenig.priv.at

Перевод на русский язык

Николай Малых

nmalykh@gmail.com