ОТЧЕТ
ПО РЕЗУЛЬТАТАМ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

ПАРАМЕТРЫ ПРОТОКОЛА ДИФФИ-ХЕЛЛМАНА, ИСПОЛЬЗУЕМЫЕ TLS-СЕРВЕРАМИ HTTPS РУНЕТА

Март 2017 года

ВВЕДЕНИЕ

Протокол Диффи-Хеллмана позволяет двум (и более) сторонам, используя открытый канал связи, договориться об общем секрете (то есть, о значении, которое известно только сторонам обмена, но не стороне, прослушивающей канал связи). Данный протокол повсеместно используется в TLS для выработки сеансовых ключей, предназначенных для защиты трафика с помощью симметричного шифра. Параметры Диффи-Хеллмана (далее - DH), для сессии в TLS определяются сервером, а клиент принимает или не принимает серверные параметры. В версиях 1.0, 1.1, 1.2 TLS допускает "статический" вариант передачи сеансового секрета: клиент шифрует его при помощи асимметричного ключа (RSA), предоставленного сервером в составе сертификата. Схема с RSA встречается на практике, в том числе, для серверов Рунета. Например, её использует веб-интерфейс системы дистанционного банковского обслуживания "Сбербанка"[1]. Также существует исторический "статический" вариант протокола Диффи-Хеллмана, в котором открытый ключ (и параметры) зафиксированы в сертификате сервера; этот вариант на практике не используется. Ни использование RSA в режиме шифрования, ни статический DH не соответствуют современным требованиям по степени защищенности, поэтому рекомендуемой настройкой TLS является согласование ключей по протоколу Диффи-Хеллмана в "динамическом" варианте. То есть, ключи вырабатываются для каждого сеанса индивидуально.

В настоящее время[2] протокол применяется в двух реализациях: классической и эллиптической. Первый, классический, вариант использует мультипликативную группу кольца вычетов; второй - группу точек эллиптической кривой. Варианты эквивалентны не только по схеме протокола, но и по фундаментальным свойствам операций. Отличаются они разрядностью чисел: для мультипликативной группы рекомендуемая разрядность модуля - 2048 бит и больше; для эллиптической кривой[3] - 256 бит и больше.

1 https://online.sberbank.ru
2 2017 год
3 Речь идёт о разрядности соответствующего конечного поля

ВЫБОРКА ДАННЫХ

Для исследования взяты данные фазы установления TLS-соединения, сообщение ServerKeyExchange, содержащее параметры DH сервера, для узлов, адресуемых доменами .RU, .SU, .РФ (A-записи) и доступных для TCP-соединения на номер порта 443 (HTTPS).

РЕЗУЛЬТАТЫ

Первым базовым классифицирующим признаком настроек DH TLS-сервера является тип группы. По этому типу выделяется классический протокол DH и эллиптический - ECDH. Для классического варианта необходимо задать модуль P - является простым числом и определяет используемую группу. В эллиптическом случае, группа определяется в параметрах типовой, именованной кривой. Реестр типовых групп (ранее - реестр кривых) ведёт IANA[4].

Месяц опроса	Общее число имён, указывающих на TLS-узлы	Число имён, указывающих на TLS-узлы, использующие DH	Число имён, указывающих на TLS-узлы, использующие ECDH	Доля ECDH от общего числа имён
мар.16	1 426 453	345 130	1 026 230	71,94%
сен.16	1 472 323	295 180	1 133 772	77,01%
мар.17	2 500 936	225 524	2 125 352	84,98%

Таблица 1. Распространённость различных типов DH в Рунете

Из таблицы 1 видно, что доля (и число) узлов, поддерживающих классический вариант DH, в Рунете падает. Это соответствует общей тенденции вытеснения этого типа протокола: эллиптический вариант считается более современным и стойким (стойкость не доказана); также преимуществом является то, что параметры ECDH имеют меньшую разрядность, требуют меньше байтов для передачи.

TLS позволяет генерировать индивидуальный модуль для TLS-сервера - это является рекомендуемым вариантом, так как для типовых модулей малой разрядности (<=1024 бит) возможны атаки, основанные на предвычисленных для известного модуля таблицах. Тем не менее, распространены случаи использования типовых модулей. Обычно их значения заданы в той или иной криптографической библиотеке, используемой на сервере.

[4] https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8

Дата	Номер значения модуля (позиция рейтинга)										Всего имён с DH
	1	2	3	4	5	6	7	8	9	10	
мар.16	179 857	135 185	10 741	9 100	7 311	482	275	265	183	131	345 130
сен.16	136 310	131 201	10 720	7 526	6 925	287	256	184	111	89	295 180
мар.17	109 391	80 794	8 547	7 453	7 326	1 214	765	751	713	662	225 524

Таблица 2а. Рейтинг TOP-10 по числу имён, указывающих на узлы, которые используют общее значение модуля DH

В таблице 2а дан рейтинг по числу доменных имён, указывающих на узлы, которые используют одно и то же значение модуля для классического DH. Приводится число имён, указывающих на узлы, которые в сообщении ServerKeyExchange предложили одно и то же значение модуля DH. Из таблицы видно, что использование одинаковых значений модулей на разных серверах является достаточно распространённой практикой: если бы подавляющее большинство серверов использовали уникальные значения модулей, то числа, соответствующие наиболее распространённым значениям, отличались бы не так существенно.

Дата	Номер значения модуля (позиция рейтинга)										Всего узлов с DH
	1	2	3	4	5	6	7	8	9	10	
мар.16	20 589	8 409	1 654	774	531	111	63	58	52	51	32 719
сен.16	15 998	7 033	1 408	818	491	106	62	47	46	33	26 463
мар.17	12 753	5 263	1 126	915	314	157	83	40	36	36	21 174

Таблица 2б. Рейтинг TOP-10 по уникальным IP-адресам узлов с одинаковыми значениями модуля DH

Распределение подтверждают данные по уникальным IP-адресам TLS-узлов (табл. 2б).

Свыше 99% серверов, поддерживающих классический вариант DH, используют в качестве генератора число 2.

С реализацией классического DH связана разрядность модуля - это число битов, необходимое для записи значения модуля. Модули малой разрядности соответствуют меньшей стойкости обмена DH. Рекомендуемым значением является 2048 бит.

Дата	Разрядность (биты)					Всего имён с DH
	> 4096	4096	2048	1024	< 1024	
	число имён (узлы по IP)					
мар.16	16 (2)	787 (102)	8 492 (974)	335 710 (31 592)	68	345 130
сен.16	12 (2)	588 (123)	7 968 (1 029)	286 519 (25 285)	51 (38)	295 180

Дата	Разрядность (биты)					Всего имён с DH
	> 4096	4096	2048	1024	< 1024	
	число имён (узлы по IP)					
мар.17	0 (0)	9707 (305)	8 752 (1 114)	206 982 (19 768)	38 (26)	225 524

Таблица 2в. Число имён и узлов по разрядности модуля классического DH

В таблице 2в приведено количество имён (и узлов), для которых использовался модуль той или иной разрядности. Подавляющему большинству имён (узлов) соответствуют модули стандартной разрядности, при этом максимальное распространение - у 1024-разрядных модулей. Такая разрядность сейчас считается недостаточной. Отметим, что при использовании уникальной группы (то есть группы, которая не относится к заранее известным типовым), разрядность 1024 бита всё ещё обеспечивает практическую стойкость, так как универсальных общедоступных методов «взлома» для 1024-битной ещё группы не предложено. Однако, если узел сейчас использует уникальную группу разрядностью 1024 бита, то следует исходить из предположения, что защищаемые данные могут утратить конфиденциальность в течение трёх-пяти лет, из-за появления эффективных атак. Разрядность, равная рекомендуемой (2048) или превышающая её - на втором месте по числу имён и узлов.

Классифицирующим признаком настроек DH сервера для эллиптического случая является используемая типовая кривая. Вместо типовой именованной кривой в TLS версий <=1.2 также возможно использовать индивидуальную кривую. Но такие решения на практике не встречаются, так как применение нетиповой кривой не рекомендуется соответствующими RFC (4492, 6460).

Самой распространённой кривой на TLS-серверах Рунета является secp256r1 (мы используем обозначения OpenSSL; эта же кривая - NIST P-256). Фактически, secp256r1 - основная кривая: она используется для более чем 95% имён, указывающих на TLS-серверы. Соответственно, две других встречающихся кривых - secp521r1 и secp384r1 - составляют минимум. Всего различных кривых обнаруживается три - см. таблицу 3.

Кривая (индекс)	Число имён, указывающих на соответствующие TLS-узлы, март 2017
secp256r1 (0x0017)	2 100 109
secp384r1 (0x0018)	17 082
secp521r1 (0x0019)	8 171

Таблица 3. Используемые кривые ECDH

ВЫВОДЫ

Показатели использования протокола Диффи-Хеллмана в Рунете отражают общее проникновение технологий защиты информации. Растёт распространение "эллиптического" варианта протокола (ECDH), это объясняется двумя факторами: 1) данный вариант имеет статус рекомендуемого практически во всех современных инструкциях по настройке TLS для системных администраторов; 2) ECDH используется массовыми хостингами.

Вместе с тем, сохраняется традиция использования типовых значений модуля DH в классическом варианте - скорость вытеснения типовых групп сравнима со скоростью вытеснения самого классического варианта протокола. При этом большое число узлов использует типовые модули малой разрядности (1024 бита), что, в модели угроз, включающей сильного игрока с большими вычислительными возможностями, представляет потенциальную уязвимость. Данная угроза скорее теоретическая, однако распространённость 1024-битных типовых модулей свидетельствует и о том, что существенное число TLS-узлов настроены без должного внимания к параметрам, то есть, могут содержать другие уязвимости, в том числе, прямо не связанные с TLS. Заведомо уязвимые модули DH (<1024 бита) - встречаются в единичных случаях.

В целом, использование протокола Диффи-Хеллмана в TLS (для HTTPS-узлов) в Рунете соответствует глобальным тенденциям, не стандартных случаев не выявлено.