БЕЗОПАСНОСТЬ
информационных технологий
ФОРУМ - САНКТ-ПЕТЕРБУРГ

Проблема автоматической классификации TLS-сессий с использованием цифровых отпечатков реализаций

Ишкуватов Сергей Маратович

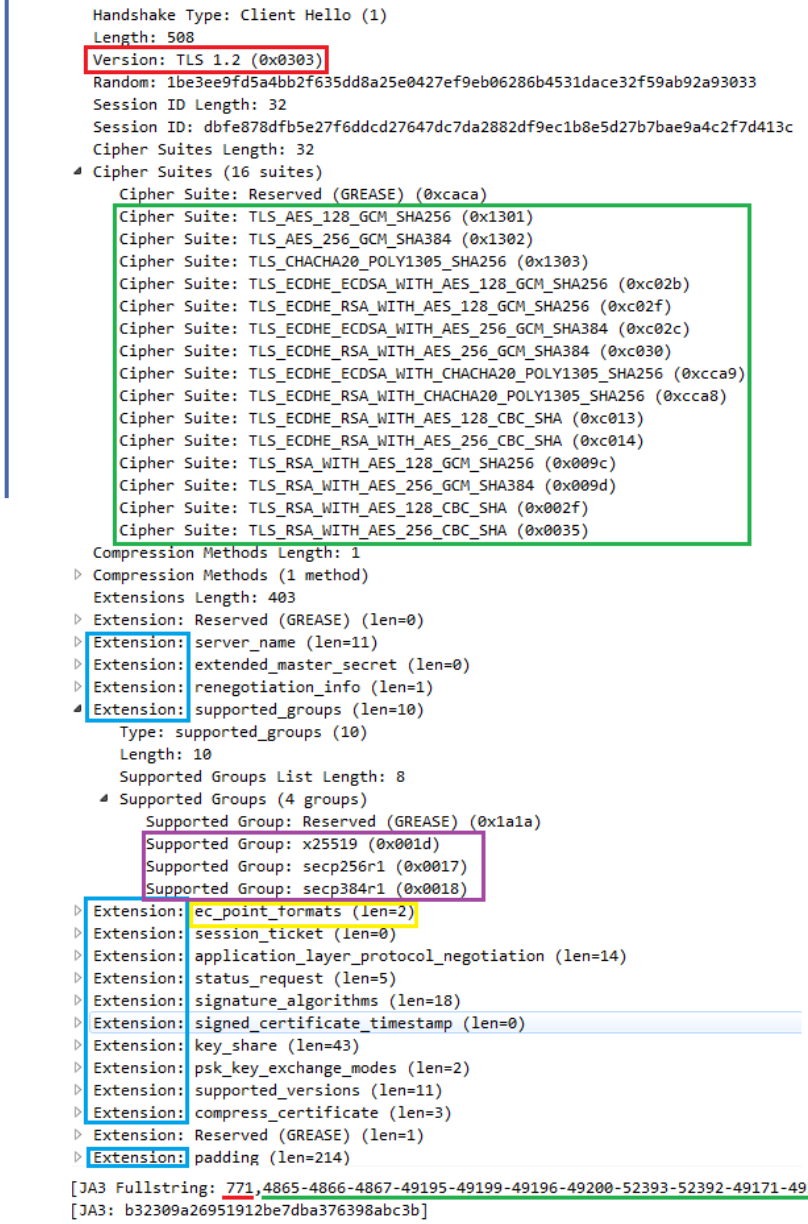
Классификация TLS-сессий по цифровым отпечаткам реализаций протоколов является важным инструментом мониторинга сетевой безопасности по следующим причинам:

1. Помогает выявить аномалии и необычную активность, которая может быть связана с атаками или нарушением безопасности в сети.
2. Обнаружение фактов использования уязвимого ПО.
3. Обнаружение фактов использования ПО запрещенного администратором сети. Обнаружение фактов использования средств анонимизации.
4. Обнаружение атак типа "Man-in-the-Middle".

Классификация TLS-сессий возможна по:

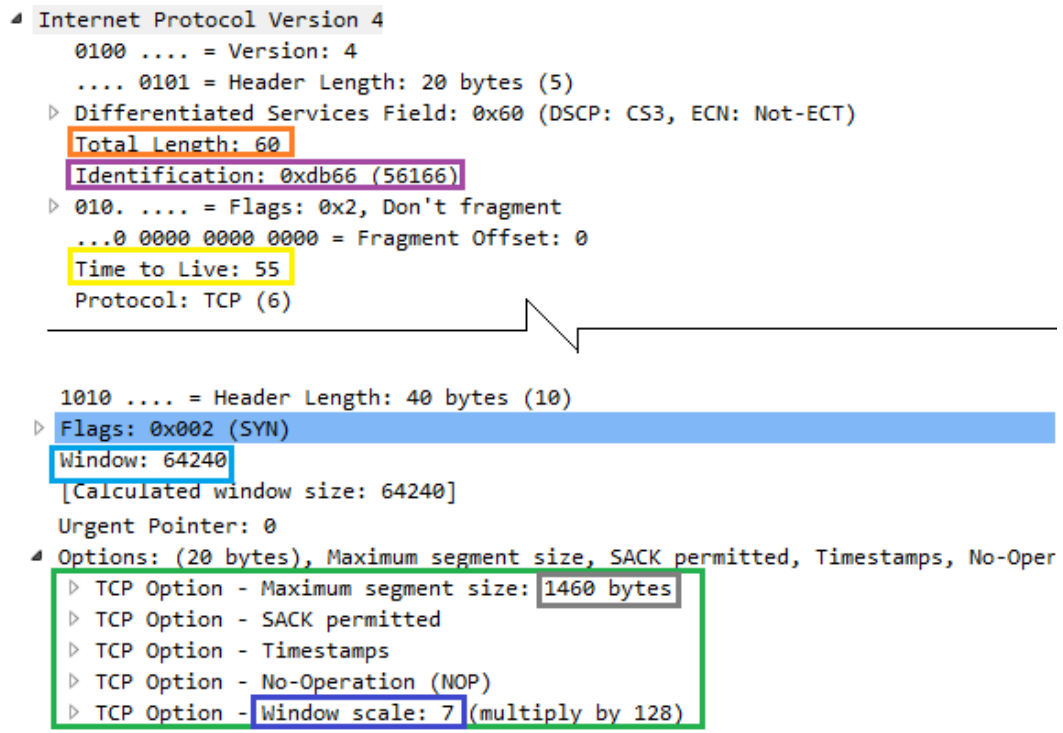
- Конечные точки Extension ServerName (если используется)
- ServerName сертификата сервера
- Диапазоны IP-адресов сервера
- Цифровой отпечаток(ЦО) клиентской реализации TLS протокола (например JA3) + цифровой отпечаток TCP/IP

Используются в качестве признаков для блокировок РКН



Что такое цифровой отпечаток реализации TLS

Под термином цифровой отпечаток реализации протокола TLS понимаются параметры, характеризующие именно эту конкретную реализацию протокола, конкретную версию библиотеки реализующий этот протокол (например Chromium, Android, .NET, Java) или группу возможных версий.



Цифровой отпечаток TCP/IP

Под термином цифровой отпечаток TCP/IP понимаются параметры, определяемые ОС источника и маршрутом следования пакета.

Наиболее популярные базы данных признаков

Цифровые отпечатки TCP/IP:

- p0f – устарела;
- satori – обновляется, не учитывает связь MTU и TCP Maximum Segment Size;
- Nmap - только для ответов серверов, рассчитан на серю активных экспериментов.

Цифровые отпечатки реализации TLS:

- JA3 – получила массовое распространение(Wireshark, Suricata, сервисы мониторинга ботнетов);
- Cisco Mercury – наиболее крупная открытая(~6000 записей), но больше не обновляется;
- Lee Brothers – устарела, обобщает классы реализаций.

Недостатки существующих представлений

- в качестве информативных признаков используют только данные начального TLS-рукопожатия, но не описывают закономерности и типичные сценарии приёма/передачи;
- учитываются только четкие совпадения признаков;
- реализация TLS веб-браузера Chromium начиная с недавнего времени случайным образом перемешивает список Extensions, в результате чего ЦО одной из последних версий даёт факториал 14 возможных вариаций записи для одной реализации.

Решение проблемы учета только четких совпадений признаков

- $$lev(a,b) = \begin{cases} |a|, \text{если} |b| = 0 \\ |b|, \text{если} |a| = 0 \\ lev\big(tail(a), tail(b)\big), \text{если } a[0] = b[0] \\ 1 + min \begin{cases} lev(tail(a), b) \\ lev\big(a, tail(b)\big) \\ lev\big(tail(a), tail(b)\big) \end{cases} \text{, в остальных случаях} \end{cases}$$

$$distance(a,b) = \sum_{i=0}^{n} s_i \ \Delta_i(a,b)$$

n – количество возможных параметров ЦО, по которому производится сравнение;
$\Delta_i(a,b)$ – количественное значение отличия i-го параметра отпечатков a и b;
s_i – информативность i-го параметра.

Расстояния Левенштейна для оценки близости цифровых отпечатков JA3

Искомый ЦО

Найденные ЦО соседи

Finger	ΔVer	ΔCS	ΔExt	ΔSuppGro	ΔPtF	∑Δ
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0						**0**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27,29-23-24,0	0	0	1	0	0	**1**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21-41,29-23-24,0	0	0	1	0	0	**1**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-41,29-23-24,0	0	0	1	0	0	**1**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	0	0	1	0	0	**1**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27,29-23-24,0	0	0	2	0	0	**2**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21-41,29-23-24,0	0	0	2	0	0	**2**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,,,	0	2	0	0	0	**2**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	0	2	0	0	0	**2**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	0	3	0	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-17513-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21-41,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-219,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-22,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-41,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-44510,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	0	2	1	0	0	**3**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27-41,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-42-43-27-41,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-10833,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-21-41,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-41,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-41,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-30032-51-45-43-27-21,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27,29-23-24,0	0	2	2	0	0	**4**
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21-41,29-23-24,0	0	2	2	0	0	**4**

Суммарное расстояние до искомого

Решение проблемы перемешивания параметров реализациями Google

Для всех реализаций, содержащих значения GREASE(Generate Random Extensions And Sustain Extensibility), перед хешированием сортировать список Extensions. Это позволит сохранить совместимость новых записей со всеми старыми записями, практически не увеличивая риски возникновения коллизий и позволит описать все возможные комбинации.

Спасибо

Контактные данные

Ишкуватов Сергей Маратович

sysroot0@gmail.com

+79062511672

САНКТ-ПЕТЕРБУРГ, 05.10.2023