Расширение `application_layer_protocol_negotiation` (ALPN) TLS

Протоколы прикладного уровня все чаще инкапсулируются в протокол TLS. Инкапсуляция позволяет приложениям использовать существующие безопасные каналы связи, уже присутствующие на порту 443, практически во всей глобальной IP-инфраструктуре. Когда несколько прикладных протоколов поддерживаются с одним номером порта на стороне сервера, например портом 443, клиент и сервер должны согласовать прикладной протокол для использования с каждым соединением. Желательно выполнить это согласование без добавления сетевых циклов между клиентом и сервером, так как каждый цикл будет ухудшать работу конечного пользователя. Кроме того, было бы выгодно разрешить выбор сертификата на основе согласованного прикладного протокола.

Расширение ALPN TLS позволяет прикладному уровню согласовывать выбор протокола в рамках Handshake TLS. При использовании ALPN клиент отправляет список поддерживаемых протоколов приложений в составе сообщения TLS ClientHello. Сервер выбирает протокол и отправляет выбранный протокол как часть сообщения TLS ServerHello. Таким образом, согласование протокола приложения может быть выполнено в рамках Hanshake TLS без добавления сетевых круговых обходов и позволяет серверу при желании связать другой сертификат с каждым протоколом приложения.

Так, определен новый тип расширения ("application_layer_protocol_negotiation"(16)), который может быть включен клиентом в его сообщение "ClientHello":

```
enum {
    application_layer_protocol_negotiation(16), (65535)
  } ExtensionType;
```

Поле «extension_data» расширения («application_layer_protocol_negotiation(16)») должно содержать значение «ProtocolNameList»:

```
opaque ProtocolName<1..2^8-1>;
  struct {
    ProtocolName protocol_name_list<2..2^16-1>
  } ProtocolNameList;
```

Серверы, которые получают сообщение ClientHello, содержащее расширение «application_layer_protocol_negotiation», могут вернуть клиенту ответ о выборе подходящего протокола. Сервер будет игнорировать любое имя протокола, которое он не распознает. Новый тип расширения ServerHello ("application_layer_protocol_negotiation(16)") может быть возвращен клиенту в расширенном сообщении ServerHello. Поле «extension_data» расширения («application_layer_protocol_negotiation(16)») структурировано так же, как описано выше для клиента «extension_data», за исключением того, что «ProtocolNameList» должен содержать ровно одно «ProtocolName».

В отличие от многих других расширений TLS, расширение ALPN не устанавливает свойства сеанса, а только соединения. Когда используются возобновление сеанса, предыдущее содержимое этого расширения не имеет

значения, и учитываются только значения в новых сообщениях подтверждения.

Ожидается, что сервер будет иметь список протоколов, которые он поддерживает, в порядке предпочтения, и выберет протокол только в том случае, если клиент его поддерживает. В этом случае сервер должен выбрать наиболее предпочтительный протокол, который он поддерживает и который также рекламируется клиентом. В случае, если сервер не поддерживает протоколы, которые объявляет клиент, сервер должен ответить фатальным Alert «no_application_protocol»:

```
enum {
    no_application_protocol(120),
    (255)
  } AlertDescription;
```

Протокол, указанный в типе расширения «application_layer_protocol_negotiation» в ServerHello, должен быть окончательным для соединения до тех пор, пока не будет проведено повторное согласование. Сервер не должен отвечать по выбранному протоколу и впоследствии использовать другой протокол для обмена данными приложения.

Расширение ALPN предназначено для использования в типичном дизайне расширений протокола TLS. В частности, согласование полностью выполняется в рамках приветственного обмена клиент/сервер в соответствии с установленной архитектурой TLS. Расширение «application_layer_protocol_negotiation» ServerHello предназначено для определения соединения (до повторного согласования соединения) и отправляется в виде открытого текста, чтобы позволить сетевым элементам предоставлять дифференцированное обслуживание для соединения, когда номер порта TCP или UDP не является окончательным для приложения. - протокол уровня, который будет использоваться в соединении. Передавая право выбора протокола серверу, ALPN упрощает сценарии, в которых выбор сертификата или перенаправление соединения могут основываться на согласованном протоколе.

Наконец, управляя выбором протокола в открытом виде как часть Handshake, ALPN избегает введения ложной уверенности в возможности скрыть согласованный протокол до установления соединения. Если требуется скрытие протокола, предпочтительным методом будет повторное согласование после установления соединения, которое обеспечит настоящие гарантии безопасности TLS.