Верификация свойств безопасности протокола SSL

Борхаленко В.А., *аспирант*
НИУ «МЭИ», г. Москва

Наиболее полная трактовка свойств безопасности протоколов описана в документах международной организации Internet Engineering Task Force [1]. Некоторые из данных свойств (G1, G7, G12, G15, G16, G20) были формализованы с помощью логики LTL [2] и верифицированы на формальной модели протокола SSL, созданной с помощью средства SPIN, функционирующей в среде с нарушителем, описываемой расширенной моделью Долева-Яо [2]. Приведем трассы, ведущие к нарушению свойств: G15 - ограниченная защищенность от атак типа «отказ в обслуживании», G16 - инвариантность отправителя и G20 - безопасное временное свойство. Свойство G20, в данной работе, утверждает, что всегда после посылки сервером сообщения в SSL-сеансе когда-нибудь в будущем клиент получит это сообщение.

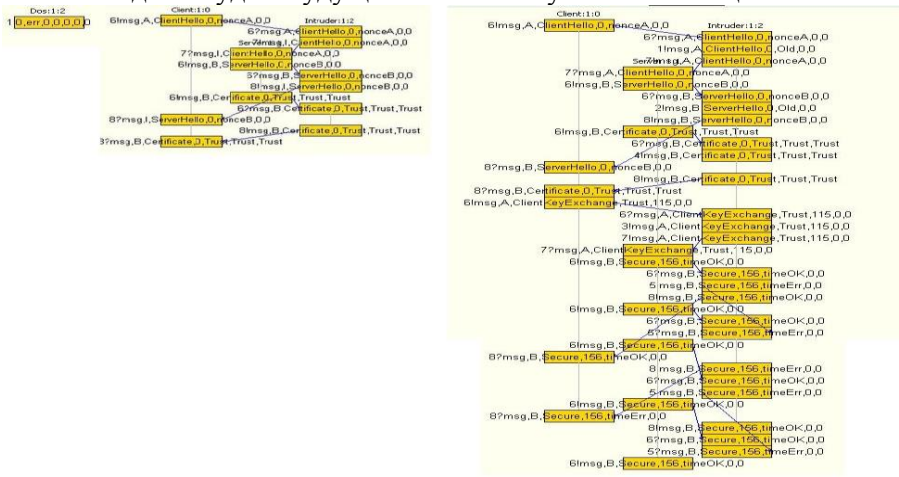

Рисунок 1 – Трассы, ведущие к нарушению свойств G15, G16, G20.

1. А.В. Черемушкин, *Криптографические протоколы: основные свойства и уязвимости* (Москва: Академия: 2009).
2. В.А. Борхаленко, *Естеств. и мат. науки в соврем. мире*, No**25**, 65 (2015).