Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.75 DOI 10.17223/2226308X/8/29

О ЗАЩИЩЁННОМ РАСПРЕДЕЛЁННОМ ПРОТОКОЛЕ В КОНКУРЕНТНОЙ СРЕДЕ НА ПРИМЕРЕ ПРОВЕДЕНИЯ СОРЕВНОВАНИЙ CTF

Н. И. Анисеня

Демонстрируется возможность создания и применения распределённого протокола в конкурентной среде на примере разработки математического метода проведения соревнований CTF (Captur The Flag), основанных на решении заданий, при угрозе DDoS-атак на сервер организаторов. Предлагается распределённый протокол проведения соревнований, который перекладывает часть функций организаторов на участников. Участники соревнования конкурируют друг с другом и не хотят помогать командам-соперникам, поэтому к протоколу предъявляются требования устойчивости к атакам со стороны самих участников. Предложенный протокол удовлетворяет поставленным требованиям. Рассмотрены атаки на протокол, исследована его устойчивость к ним, предложены модификации протокола. Сообщается о возможных направлениях дальнейших исследований в данной области.

Ключевые слова: *распределённые протоколы, защищённые вычисления, отказоустойчивые системы.*

Цель работы — предложить математический способ обеспечения доступности соревнования CTF, проводимого в формате Jeopardy, при угрозе DDoS-атаки на организаторов.

Под *централизованным сетевым взаимодействием*, или просто *централизованным взаимодействием*, участников будем понимать такое их взаимодействие, которое полагается на некоторый известный всем участникам узел сети — посредника, имеющего отличную от прочих участников и незаменимую по отношению к ним роль.

Злоумышленником назовём нечестного участника соревнования, который преследует хотя бы одну из следующих целей:

1) нарушение работоспособности системы, с высокой вероятностью приводящее к невозможности участия в соревновании всех участников;
2) нарушение работоспособности системы, с высокой вероятностью приводящее к искажению собственных результатов;
3) нарушение работоспособности системы, с высокой вероятностью приводящее к искажению результатов другого конкретного участника.

Активным участием некоторого узла назовём такое его поведение в сети, при котором он отправляет в сеть данные.

Для достижения указанной цели ставится следующая задача: разработать протокол распределённого проведения соревнований CTF, основанных на решении заданий.

Требования к протоколу следующие:

1) в результате работы протокола должна формироваться таблица результатов, позволяющая восстановить очерёдность получения ответов;
2) протокол не должен требовать активного участия организаторов во время проведения соревнования;
3) протокол не должен полагаться на централизованное взаимодействие участников во время проведения соревнования;
4) протокол должен позволять проводить соревнование даже при отключении большого количества участников;
5) протокол должен позволять проводить соревнование даже при большом количестве злоумышленников (нечестных участников).

При разработке протокола не рассматривались следующие ситуации и проблемы:

1) проблемы подготовительного этапа (регистрации команд);
2) ситуация распада графа сети на компоненты связности;
3) недостаточная точность временных расчётов с учётом выбранного временного окна.

Пусть на момент начала соревнования имеется сеть участников, описанная в [1], в которую команда организаторов входит как равноправный участник. Полагаем, что в этой сети для передачи сообщений используется безотказная луковая маршрутизация, описанная в [1]. Каждый участник на момент начала соревнования имеет:

1) алгоритмы цифровой подписи sign и verify;
2) алгоритм симметричного шифрования на ключе E_x;
3) множество идентификаторов участников U;
4) ключи проверки ответов $g_1, \ldots, g_m$;
5) псевдослучайную функцию $G(y)$ с параметрами k, t;
6) зашифрованный набор заданий.

Началом соревнования считается момент рассылки организаторами ключа для расшифрования списка заданий, после чего команда организаторов перестаёт принимать активное участие.

Пусть некоторый участник u с идентификатором ID_u получил ответ f на задание. Рассмотрим протокол, согласно которому должен действовать участник u:

1) $y = \mathrm{sign}_f(t_u, ID_u)$, t_u — текущее время пользователя u.
2) Для всех пользователей с идентификатором $id \in G(y)$:
   а) $u \to id : z = E_x(y, t_u, ID_u)$, x — сеансовый ключ;
   б) $id \to u : t_{id}, \mathrm{sign}_{\widehat{id}}(z, t_{id})$, t_{id} — текущее время пользователя с идентификатором id.
3) Каждому пользователю с идентификатором $id \in U$ выслать:
   t_u, ID_u, $y = \mathrm{sign}_f(t_u, ID_u)$, $z = E_x(y, t_u, ID_u)$, x, $\{t_i, \mathrm{sign}_{\widehat{id_i}}(z, t_i) : i \in G(y)\}$.

Соревнование завершается в установленное организаторами время. Таблица результатов, имеющаяся у организаторов в этот момент, считается итоговой.

Атаки, улучшения и дальнейшие направления исследований описаны в [1].

ЛИТЕРАТУРА

1. *Анисеня Н. И.* Разработка безопасного протокола распределённой системы проведения соревнований CTF // Прикладная дискретная математика. 2015. № 2(28). С. 59–70.