ЛОГИКА МОДЕЛИРОВАНИЯ ВРЕМЕНИ В КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛАХ

Даминов А.А.
стажёр-учитель, Ташкентский Университет Информационных Технологий, (akmalbekdaminov1998@gmail.com)
https://doi.org/10.5281/zenodo.11532644

ARTICLE INFO

Qabul qilindi: 01-June 2024 yil
Ma'qullandi: 04- June 2024 yil
Nashr qilindi: 08- June 2024 yil

KEY WORDS

BAN логика, аутентификаци, дискретное время, криптографические протоколы, тайм-релиз, анализ.

ABSTRACT

В данной статье предложена логика для моделирования времени в криптографических протоколах. В большинстве существующих логик время не учитывается, несмотря на его важную роль в протоколах. В предложенной логике время используется как параметр предикатных и модальных операторов, что позволяет моделировать действия, знания и убеждения агентов в разные моменты времени. Приводится метод анализа криптографических протоколов с учетом временного фактора, что особенно полезно для анализа протоколов, зависящих от времени.

Время играет важную роль в криптографических протоколах. Протоколы представляют собой последовательность действий, выполняемых во времени, и некоторые из них имеют требования, зависящие от времени. Например, в аспекте секретности агенты могут требовать, чтобы определенные сообщения оставались секретными до определенного времени. В аспекте аутентификации состояние убеждений агентов может изменяться со временем. Поэтому при анализе криптографических протоколов необходимо учитывать временной фактор.

Логика, разработанная Бэрроузом, Абади и Нидэмом (BAN логика), быстро стала широко используемым формальным методом анализа криптографических протоколов. Однако в этой логике время не используется явно, что делает её неподходящей для анализа протоколов, зависящих от времени. Логика, предложенная Коффи и Саидха, использует время, но она ориентирована на анализ протоколов с открытым ключом для решения задач аутентификации. Для анализа временно-зависимых криптографических протоколов её необходимо расширить.

Предложенная логика

Язык логики

Логика основана на предикатной модальной логике и включает четыре типа переменных: агенты (A), дискретное время (T), ключи (K) и сообщения (M).

Определения

Константы

- e: специальный агент, представляющий все факторы окружающей среды,

включая атакующих.

- T_0: начальное время выполнения протокола.

Переменные

- τ,τ',τ'', ...: переменные типа T.
- i,j,i',j': переменные типа A.
- k,k',k'', ...: переменные типа K.
- m,m',m'', ...: переменные типа M.

Функции

- AgtPrivate:A→K: функция частного ключа агента.
- AgtPublic:A→K: функция открытого ключа агента.
- ShareKey:A×A→K: функция общего ключа.
- TimePrivate:T→K: функция временного частного ключа.
- TimePublic:T→K: функция временного открытого ключа.
- Cmb:M×M→M: функция комбинированного сообщения.
- EncDec:M×K→M: функция шифрования или дешифрования.
- Reverse:K→K: функция обратного ключа.Plus:T×T→T: функция суммы времени.

Предикаты

- (m): сообщение mmm является свежим.
- $\tau \leq \tau'$: время τ предшествует времени τ'.
- C(m,m′): сообщение mmm содержит сообщение m′.
- G(i,m,m′,τ): агент i может получить сообщение m′ из сообщения m в момент времени τ.
- S(i,m,τ): агент i отправляет сообщение mmm в момент времени τ.
- R(i,m,τ): агент i получает сообщение mmm в момент времени τ.
- H(i,m,τ): агент i держит сообщение mmm в момент времени τ.

Аксиомы и правила вывода

1. Аксиомы предикатной логики.
2. Формула Баркана:
   - $(\forall x)Bi(\tau)\phi \leftrightarrow Bi(\tau)(\forall x)\phi$.
   - $(\exists x)Bi(\tau)\phi \leftrightarrow Bi(\tau)(\exists x)\phi$.
3. Аксиомы монотонности:
   - Если агент держит сообщение (или верит в утверждение), он будет держать (или верить) его и далее.
4. Аксиомы времени:
   - Время рефлексивно и транзитивно.
5. Аксиомы ключей:
   - Свойства ключей, включая приватные и публичные ключи.
6. Аксиомы получения сообщения:
   - Агенты могут получать сообщения из других сообщений при выполнении определённых условий.
7. Аксиомы содержания:
   - Отношения содержания между сообщениями.
8. Аксиомы действий:

- Если агент получает сообщение, для каждой части этого сообщения должен существовать агент, который держит и отправил сообщение, содержащее эту часть

Пример анализа протокола

Для демонстрации предложенного метода используется протокол тайм-релиза, предложенный Михихару Кудо и Аниш Матуиа. Протокол имеет трех участников: Алиса (A), Боб (B) и Трент (T). Алиса хочет отправить временно-конфиденциальное сообщение в будущее, Боб является получателем, а Трент — доверенной третьей стороной, способной генерировать асимметричные временные пары ключей и связывать приватный ключ с конкретным моментом времени.

Описание протокола

1. Алиса отправляет Тренту запрос на генерацию ключа.
2. Трент генерирует временной ключ и отправляет его Алисе.
3. Алиса шифрует сообщение временным ключом и отправляет его Бобу.
4. Боб отправляет Алисе nonce.
5. Алиса комбинирует nonce с сообщением и отправляет Бобу.
6. Боб отправляет запрос Тренту на дешифрование сообщения.
7. Трент проверяет текущее время и, если оно соответствует, отправляет Бобу приватный ключ для дешифрования.

Анализ протокола

1. Связь времени с каждым шагом протокола.
2. Формализация протокола в виде набора формул.
3. Задание начальных предположений.
4. Формулирование целей криптографического протокола.
5. Доказательство целей с использованием предложенной логики.

Заключение. В статье предложена логика, основанная на предикатной модальной логике, для моделирования времени в криптографических протоколах. Приведен пример анализа тайм-релизного протокола, который демонстрирует эффективность предложенного подхода для анализа временно-зависимых свойств, таких как секретность и аутентификация. Дальнейшие исследования могут быть направлены на применение предложенной логики для анализа различных криптографических протоколов и изучение возможности её использования для анализа справедливости протоколов, особенно с временными ограничениями.

Список литературы:

1. Rivest RL, Shamir A, Wagner DA, “Time-Lock Puzzles and Timed-Release Cryptographic protocol,” Technical Report, MIT/LCS/TR-684, Cambridge:MIT Laboratory for Computer Science, 1996.
2. Péter T, “The Additional Examination of the Kudo-Mathuria Time-Release Protocol,” Journal of Universal Computer Science, 2006, 12(9):1373-1384.
3. Zhang Y, Varadharajan V, “A Logic for Modeling the Dynamics of Beliefs in Cryptographic Protocols”. In: Michael O, Proceedings of 24th Australasian Computer Science Conference, Washington DC: IEEE Computer Society, 2001. 215-222.
4. Burrows M, Abadi M, Needham R, “A Logic of Authentication,” In: Proceedings of the Royal Society of London A, Vol 426. 1989. 233-271.
5. Gong L, Needham R, Yahalom R, “Reasoning about Belief in Cryptographic Protocols,” In:

Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1990. 234-248.
6. Abadi M, Tuttle MR, “A Semantics for a Logic of Authentication,” In: Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing. ACM Press, 1991. 201-216.
7. Syverson PF, van Oorschot PC, “On unifying some cryptographic protocol logics,” In: Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and