УДК 681.3.06:519.248.681

В.Е. Чевардин, В.Г. Прокопенко

Военный институт телекоммуникаций и информатизации НТУУ «КПИ», Полтава

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ, ПЕРСПЕКТИВНЫЕ ПУТИ ИХ РАЗВИТИЯ

Введение

В наше время большую роль в информационных системах играют сетевые технологии, базирующиеся на объединении огромного числа машин в единую сеть. Одним из ярких примеров такой сети является Internet. Она основана на многопользовательских операционных системах, позволяющих управлять данными, хранящимися на удалѐнных машинах (серверах) сразу нескольким людям. Иногда требуется сделать доступной для всех только часть документов.

Основной материал

Хэш-функции являются одним из важнейших криптографических примитивов. Они используются для получения цифровых отпечатков сообщений (в том числе заверяемых электронной подписью), кодов аутентификации сообщений по симметричному ключу, генерации псевдослучайных чисел, разворачиванию ключей из входного значения и множества других протоколов. Совершенно новым этапом в развитии и реализации MAC-кодов является разработка MAC-кодов основанных на блочных шифрах, т. н. CBC-MAC, к которым относятся EMAC, RMAC, OMAC, PMAC, TMAC, XCBC.

В докладе приведены результаты исследований данных методов ключевого хеширования. Рассмотрены основные виды атак на существующие хеш-функции. Определены наиболее существенные уязвимости представленных способов хеширования. А также рассматривается возможность модернизации существующих методов и в дальнейшем разработка качественно нового метода ключевого хеширования.

Полученные в работе результаты отражают новый подход к построению ключевых схем хеширования – MAC-алгоритмов. Основой для создания новых схем послужили теоретико-сложностные задачи математики. Это дает возможность теоретически обосновать границу вероятности коллизий и получить доказуемо стойкую схему аутентификации сообщений, что не позволяют существующие алгоритмы.

Выводы

Таким образом, сейчас после нахождения коллизий в хеш-фукнциях MD4, MD5, SHA-1 и публикации теоретической работы, доказывающей возможность взлома SHA-1, Национальный Институт Стандартов и Технологий США занимается разработкой нового стандарта хеширования. Данный стандарт должен поддерживать размер выходного блока 224, 256, 384 и 512 битов. Сохраняются те же требования, что и к предыдущим хэш-функциям: максимальный размер входного значения, размер выходного значения, коллизионная стойкость, стойкость к нахождению прообраза и второго прообраза, потоковый режим вычисления "за один проход".

Перспективным является способ нахождения такого метода, который обеспечит достаточную криптостойкость при незначительном уменьшении скорости передачи.

Данное уменьшение в будущем будет одним из основных показателей применимости разработанного алгоритма.

Список литературы

1. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. – April 19, 2004 – Vers. 0,15 (beta).

3. Bellare M. Keying hash function for message authentication / M. Bellare, R. Canetti, H. Krawczyk. – 1996. – P. 1-15.

4. Black J. UMAC: Fast and provably secure message authentication / J. Black, S. Halevi, H. Krawczyk, T. Krovetz, P. Rogaway. – Springer-Verlag, 1999. – P. 216-233.