УДК 681.3.06

Б.П. Томашевский

Львовский Военный институт Сухопутных войск им. гетмана П. Сагайдачного, Львов

АНАЛИЗ МОДЕЛЕЙ АТАК ЗЛОУМЫШЛЕННИКА НА ПОДСИСТЕМУ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Рассматриваются модели осуществления атак злоумышленника на подсистему криптографической защиты информации в компьютерных системах и сетях. Приводится классификация атак и нарушителей безопасности компьютерных систем и сетей, исследуются возможности злоумышленника по реализации различных моделей атак.

Ключевые слова: *криптоатаки, классификация криптографических атак.*

Вступление

Постановка проблемы в общем виде и анализ литературы. Важным показателем эффективности современных компьютерных систем и сетей является безопасность обрабатываемой и передаваемой информации [1 – 3]. С точки зрения адекватной оценки достигаемого уровня безопасности информационных систем и технологий и выработки практических рекомендаций по совершенствованию подсистемы криптографической защиты информации актуальной задачей является анализ моделей осуществления атак злоумышленника, оценка уязвимости информационных ресурсов в компьютерных системах и сетях [1 – 6]. **Целью данной статьи** является исследование моделей осуществления атак злоумышленника на подсистему криптографической защиты информации в компьютерных системах и сетях, выявление наиболее опасных с практической точки зрения видов атак и сценариев поведения нарушителя.

Основной раздел

Модели осуществления атак злоумышленника. Проведенный анализ показал, что в самой общей классификации все атаки злоумышленника можно классифицировать следующим образом [5, 6]:

1) атака с известной кодограммой – противник имеет возможность перехватывать передаваемые по каналу связи криптограммы и посредством злоумышленных действий пытается восстановить передаваемый открытый текст и/или вычислить секретный ключ;

2) атака с подобранной кодограммой – противник имеет возможность воздействовать на передающую сторону таким образом, что по каналу связи будут передаваться наиболее удобные для криптоанализа криптограммы, после перехвата которых противник посредством злоумышленных действий пытается восстановить передаваемые информационные данные и/или вычислить секретный ключ;

3) атака с известным открытым текстом – противник имеет возможность сопоставить перехваченной криптограмме искомый открытый текст и посредством злоумышленных действий пытается вычислить секретный ключ;

4) атака с подобранным открытым текстом – противник имеет возможность воздействовать на передающую сторону таким образом, что по закрытому каналу связи будут передаваться наиболее удобные для криптоанализа открытые тексты, причем противник имеет возможность перехватывать любые криптограммы, ставить им в соответствие открытые тексты и посредством злоумышленных действий пытается вычислить секретный ключ.

В соответствии с общими положениями теории защиты информации злоумышленника можно классифицировать следующим образом [1 – 6]:

– внешний нарушитель – нарушитель, который может иметь только общедоступные данные криптографического протокола, а также иметь доступ только к открытым каналам связи;

– внутренний нарушитель – нарушитель, который кроме информации, доступной внешнему нарушителю, может располагать некоторой специфической информацией (время и режим обмена информацией, дополнительные данные, которые используются в протоколе);

– активный нарушитель – нарушитель, который при попытке раскрытия криптосистемы осуществляет активные действия, т.е. действия, при которых нарушитель во время протокола каким-либо образом влияет на данные, переданные в каналах связки;

– пассивный нарушитель – нарушитель, который выполняет атаку на протокол с помощью прослушивания канала связи и перехват всех переданных между участниками протокола сообщений и дальнейший их анализ.

На рис. 1 – 4 в общем виде приведены модели осуществления пассивных и активных атак со стороны внешних и внутренних злоумышленников.

Общая модель осуществления пассивной атаки со стороны внешнего злоумышленника представлена на рис. 1. Суть этой атаки состоит в том, что злоумышленник, определив факт передачи данных в компьютерной системе или сети связи, осуществля-

ет их перехват с целью дальнейшего анализа. При этом нарушитель может владеть открытыми параметрами и данными, которые используются участниками протокола обмена данными. Целью злоумышленника является криптоанализ протокола для определения сеансовых и/или долговременных ключевых данных.

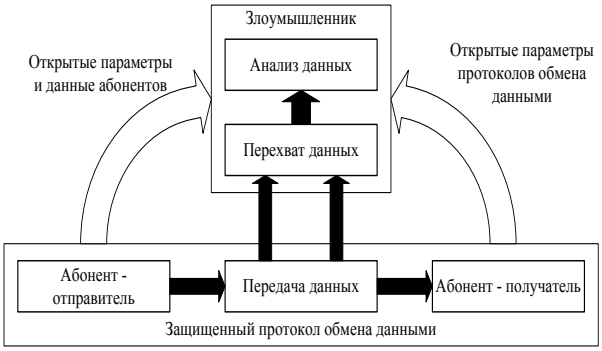

Рис. 1. Модель осуществления пассивной атаки со стороны внешнего злоумышленника

Общая модель осуществления активной атаки со стороны внешнего злоумышленника представлена на рис. 2.

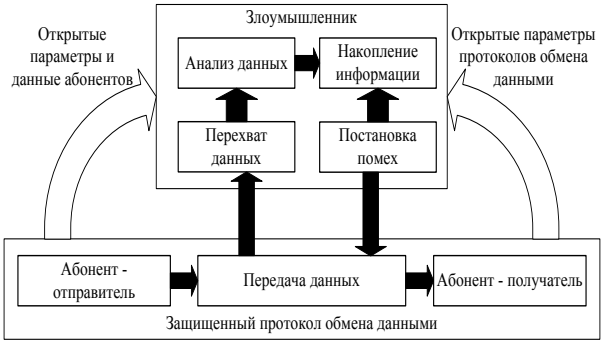

Рис. 2. Модель осуществления активной атаки со стороны внешнего злоумышленника

Суть этой атаки состоит в том, что злоумышленник, определив факт передачи данных в компьютерной системе или сети связи, осуществляет их перехват, анализ и накопление полученной информации о режимах работы системы, используемых каналах, методах согласования источников информации, и др. При этом нарушитель также может владеть открытыми параметрами и данными, которые используются участниками протокола обмена данными. Целью злоумышленника является нарушение работы системы или ее блокирование путем подачи в канал связи помехи или множества помех, действие которых может приводить к снижению качества передачи данных в защищенных протоколах обмена данными. Если в результате таких действий вероятность ошибки на один бит передаваемых данных достигает недопустимого уровня, то канал блокируется и цель злоумышленника считается достигнутой.

Общая модель осуществления активных атак со стороны внутреннего злоумышленника представлена на рис. 3, 4.

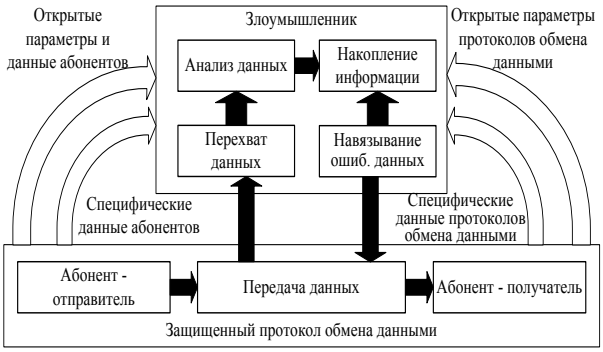

Рис. 3. Модель осуществления активной атаки со стороны внутреннего злоумышленника при навязывании ошибочных данных

Суть этих атак состоит в том, что злоумышленник, определив факт передачи данных в компьютерной системе или сети связи, осуществляет их перехват, анализ и накопление полученной информации о режимах работы системы, используемых каналах, методах согласования источников информации, и др.

При этом нарушитель также может владеть как открытыми параметрами и данными, которые используются участниками протокола обмена данными, так и некоторой специфической информацией (время и режим обмена информацией, дополнительные данные, которые используются в протоколе).

Целью злоумышленника является навязывание ошибочных ключевых данных (в протоколах формирования и обмена общих ключей), фрагментов передаваемых данных (в протоколах идентификации).

Модель такой атаки со стороны внутреннего злоумышленника представлена на рис. 3.

Другая модель осуществления активных атак со стороны внутреннего злоумышленника представлена на рис. 4, где нарушитель пытается полностью подменить собой участника информационного обмена путем имитации различных режимов передачи данных, согласования источников информации или синхронизации технических средств.

Кроме приведенных выше определений нарушителя, существуют уровни возможностей нарушителя [5, 6].

Определение уровней зависит от запланированных условий эксплуатации средств криптографической защиты информации и ценности защищаемой информации: и описывается следующим образом:

– нулевой уровень – случайное неумышленное ознакомление с содержанием информации (случайное прослушивание канала);

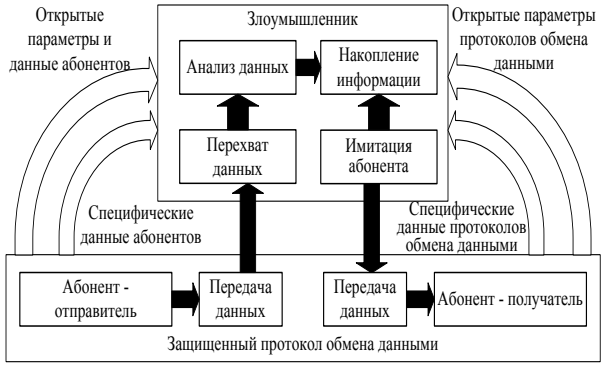

Рис. 4. Модель осуществления активной атаки со стороны внутреннего злоумышленника при навязывании ложных режимов передачи данных

– первый уровень – нарушитель имеет ограниченные средства и самостоятельно создает средства и методы атак на средства криптографической защиты информации, а также информационно-телекоммуникационные системы с применением доступных программных средств и электронно-вычислительной техники;

– второй уровень – нарушитель корпоративного типа, имеет возможность создания специальных технических средств, стоимость которых соотносится с возможным финансовым ущербом при потере, искажении и уничтожении защищаемой информации. В этом случае для распределения вычислений при проведении атак могут применяться локальные вычислительные сети;

– третий уровень – нарушитель имеет научно-технический ресурс, который приравнивается к научно-техническому ресурсу специальной службы экономически развитого государства.

Выводы

В результате проведенных исследований показано, что наиболее опасными являются внутренние нарушители, проводящие активные действия по реализации своих атак. С точки зрения возможностей злоумышленника наиболее опасными следует считать атаки с подобранным открытым текстом, когда противник имеет возможность перехватывать любые криптограммы, ставить им в соответствие открытые тексты и посредством злоумышленных действий пытается вычислить секретный ключ.

Перспективным направлением является дальнейшие исследования стойкости криптографических средств защиты информации к рассмотренным атакам противника. При этом следует предполагать, что противник имеет возможность реализовать все типы атак, вплоть до четвертого – атаку с подобранным открытым текстом, при этом он может быть классифицирован как внутренний и/или внешний активный нарушитель с третьим уровнем возможностей.

Список литературы

1. Захист інформації в комп'ютерних системах від несанкціонованого доступу / за ред. С.Г. Лаптєва. – К., 2001. – 321 с.

2. Мамаев Е. Технологии защиты информации в Интернете / Е. Мамаев. – СПб.: ИД Питер, 2001. – 848 с.

3. Харин Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 382 с.

4. Мао В. Современная криптография. Теория и практика / В. Мао. – М.: «Вильямс», 2005. – 768 с.

5. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.

6. Молдавян Н.А., Молдавян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдавян, А.А. Молдавян, М.А. Еремеев. – СПб.: БХВ, 2004. – 448 с.

Поступила в редколлегию 8.12.2009

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ МОДЕЛЕЙ АТАК ЗЛОВМИСНИКА НА ПІДСИСТЕМУ КРИПТОГРАФІЧНОГО ЗАХИСТУ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Б.П. Томашевський

Розглядаються моделі здійснення атак зловмисника на підсистему криптографічного захисту інформації в комп'ютерних системах і мережах. Приводиться класифікація атак і порушників безпеки комп'ютерних систем і мереж, досліджуються можливості зловмисника за реалізацією різних моделей атак.

Ключові слова: *криптоатаки, класифікація криптографічних атак.*

ANALYSIS OF MODELS OF ATTACKS OF MALEFACTOR ON SUBSYSTEM OF CRYPTOGRAPHIC DEFENCE IN COMPUTER SYSTEMS AND NETWORKS

B.P. Tomashevskiy

The models of realization of attacks of malefactor are examined on the subsystem of cryptographic priv in the computer systems and networks. Classification over of attacks and violators of safety of the computer systems and networks is brought, possibilities of malefactor are probed on realization of different models of attacks.

Keywords: *cryptoattacks, classification of cryptographic attacks.*