Academia de Studii Economice din Moldova

17 ANI

ANALELE ACADEMIEI DE STUDII ECONOMICE DIN MOLDOVA

VI

Ministerul Educaţiei şi Tineretului al Republicii Moldova

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA

ANALELE

ACADEMIEI DE STUDII ECONOMICE DIN MOLDOVA

Ediţia aVI-a

Editura ASEM
Chişinău - 2008

CZU [33+378.6](478)(082)=135.1=161.1
A 15

DESCRIEREA CIP A CAMEREI NAȚIONALE A CĂRȚII

Academia de Studii Economice din Moldova. Analele Academiei de Studii Economice din Moldova, Ed. a 6-a / Acad. de Studii Econ. din Moldova; col. red.: Grigore Belostecinic (preş.), ... – Ch.: ASEM, 2008. – 401 p. – ISSN 1857-1433

Texte : lb. rom., rusă. – Bibliogr. la sfârşitul art.

ISBN 978-9975-75-405-7

50 ex.

- - 1. Economie. 2. Academia de Studii Economice din Moldova – Anale.

[33+378.6](478)(082)=135.1=161.1

A 15

ISBN 978-9975-75-405-7

C U P R I N S

I. MANAGEMENT ŞI MARKETING

II. PROBLEMELE GENERALE ALE ECONOMIEI NAȚIONALE

III. CIBERNETICĂ ŞI INFORMATICĂ ECONOMICĂ

IV. FINANŢE, ACTIVITATEA BANCARĂ

V. CONTABILITATE, ANALIZA ACTIVITĂŢII ECONOMICO-FINANCIARE

VI. STATISTICĂ ŞI MATEMATICĂ

cum rezultă din figura 3, relaţia este una cu legătură inversă. Legătura inversă este necesară pentru a asigura dezvoltarea şi perfecţionarea continuă a modelului mixt.

Concluzii

În rezultatul analizelor efectuate şi prezentate în prezentul articol, ipoteza posibilităţii aplicării unui model mixt de evaluare a riscurilor TI ce să rezolve mai mult sau mai puţin problemele legate de cost-eficienţa măsurilor de protecţie, este confirmată. S-a dovedit, însă, că simpla stabilire a modelului nu poate să rezolve problema cost-eficienţei tratării riscurilor. Modelul mixt poate oferi metoda de evaluare a riscurilor, nu va spune, însă, când şi cum poate fi metoda folosită. Ideea lansată în acest articol este că un meta-model poate să rezolve problema aplicării modelului. Obiectivul stabilit în faţa meta-modelului este de a aplica metodele aferente modelului mixt de evaluare a riscurilor TI, astfel încât rezultatul obţinut să fie cost-eficient şi optim pentru organizaţie. Această idee, însă, este necesar să fie suplimentar dezvoltată, constituind un bun subiect de cercetare ştiinţifică ulterioară.

Bibliografie:

1. Risk Management Guide for IT Systems, National Institute of Standards and Technologies, SP 800-30, July 2002;
2. Quantifying IT Risks, Robert Jacobson, Institute of Internal Auditors Journal, vol.5, 2002;
3. Risk Assessment for IT Security, Scott Laliberte, Bank Accounting & Finance, August 2004;
4. Risk-aware Decision Making for New IT Investments, Georges Ataya, Information Systems Control Journal, vol. 2, 2003;
5. New Basel Accord: Operational Risk Management – Emerging Frontiers for the Profession, Mohan Bhatia, Information Systems Control Journal, vol. 1, 2002;
6. Subjectivity in Risk Analysis, Felix Redmill, www.ncl.ac.uk;
7. Quantitative Risk Assessment: An Outline to being Realistically Prepared, John Crocker, www.clermiston.com.au.

АНАЛИЗ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

Проф. унив., д-р хаб. Сергей ОХРИМЕНКО
Преп. Константин СКЛИФОС

In work the review of a modern condition and use of formal methods for the analysis, designing and checks of cryptographic protocols of autentifications is resulted

Введение

Основным моментом в управлении безопасностью информационной системы является личная ответственность каждого пользователя. Это достигается с помощью использования механизмов, закрепляющих ответственность. Каждому пользователю присваивается условное имя, уникальное в данной системе, а соответственно этому имени устанавливается пароль, который пользователь должен хранить в секрете и предъявлять системе в качестве доказательства того, что он именно тот, за кого выдает себя. Таким образом, в управлении безопасностью информационной системы (ИС) и ее информационными ресурсами выделяются два механизма: идентификация, которая выражается через соответствующее условное имя, и аутентификация, которая выражается через предъявление пароля.

После аутентификации доступ пользователю к ресурсам системы разрешается в соответствии с политикой доступа, внедренной в ИС, и правами, определяемыми администратором на этапе авторизации.

Одновременно с механизмами аутентификации в ИС должны быть внедрены механизмы фиксации авторства, которые обязаны обеспечить невозможность отказа пользователя от своих действий, что обеспечивается с помощью мониторинга и аудита. В плане расследования компьютерных инцидентов данные механизмы достаточно надежны и являются инструментом анализа прошедших событий. Следует отметить, что они не обладают свойством доказательности, т.е. их нельзя применять при доказательстве авторства. Это связано, в первую очередь, с тем, что система защиты является комплексной и сложным конгломератом информационных технологий,

которые интегрированы в саму ИС. Для использования данных аудита в доказательстве авторства необходимо доказать, что сама ИС защищена, а это является сложным и трудоемким процессом. Кроме того, предполагается, что данные аудита являются на 100% верными, означающими, в свою очередь, доказательство того, что сама ИС защищена на 100%. С теоретической точки зрения создание подобных ИС возможно.

Таким образом, успешность действий по организации защиты информации имеет в качестве базового стержня аутентификацию.

Методы аутентификации

Для сравнения различных протоколов аутентификации, выявления их общих или специфических свойств, а также упорядоточения их множества, целесообразно привести систему классификации. Считаем возможным выделить следующие группы: с точки зрения места; типа аутентификации; по объектам; по типу использования заявочной информации (или по способу разделения секретов). Рассмотрим их подробнее (рис.1).

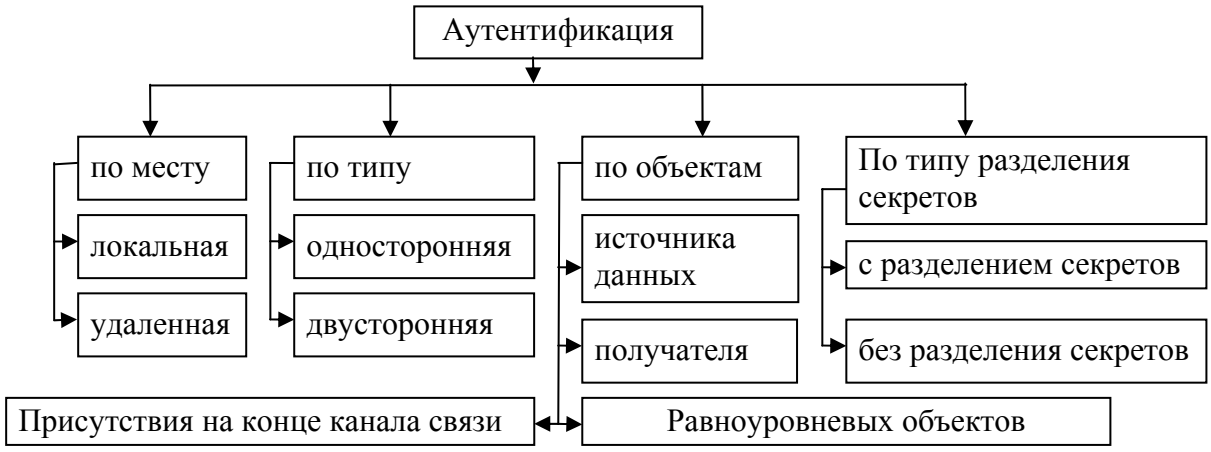

Рис.1. Классификация методов аутентификации

С точки зрения места аутентификации выделяют локальную и удаленную. Локальная означает, что аутентификация проводится непосредственно интерактирующим компьютером. В качестве примера может быть рассмотрена ситуация, в рамках которой пользователь аутентифицируется при загрузке компьютера.

При удаленной аутентификации объект или субъект, являющийся источником информации, находится на значительном расстоянии от проверяющего, разделенный каналом связи. В этом случае задача аутентификации сводится к процессу доказательства:

1) подлинности самого сообщения и/или
2) его авторства, а также
3) подлинности соединения.

По типу протокола выделяют одностороннюю и двустороннюю аутентификацию. *Односторонняя* – когда только одна сторона, запрашивающая доступ, аутентифицируется, а сторона, предоставляющая доступ, аутентифицирует. В качестве примера можно рассматривать парольную защиту, как самый распространенный на практике механизм односторонней аутентификации. *Двусторонняя (взаимная) аутентификация* – когда участники одновременно или попеременно играют роль доказывающего или проверяющего по отношению друг к другу, но по окончании протокола аутентификации они взаимно аутентифицированы.

По объектам аутентификации рассматривают: источник данных; получатель; участник протокола; способ разделения секретов.

Источник данных – доказывает авторство заявителя на данные, принятые получателем. В процессе обмена данными появляется необходимость обеспечения аутентичности источника данных и после того, как протокол аутентификации или сеанс связи даже окончен.

Объектом аутентификации может быть получатель (получатели). Некоторые протоколы позволяют аутентифицировать одного или нескольких получателей.

Использование участника протокола в качестве объекта призвано доказывать присутствие заявленного лица, объекта или процесса на другом конце канала связи. Для решения задачи

необходимо поддерживать состояние аутентичности участника в протоколе после завершения его первичной аутентификации, так как в противном случае возможно подключение нарушителя сразу после ее окончанию.

И последний классификационный признак – по способу разделения секретов:

- *с разделением секрета* – протокол аутентификации, для реализации которого необходимо, чтобы обе стороны процесса аутентификации заблаговременно обменялись секретами. Подобные протоколы имеют существенный недостаток, который заключается в проблеме первого контакта, в рамках которого и необходимо разделить секрет (пароль или ключ) для шифрования (если протокол криптографический);
- *без разделения секрета* – подобного рода протоколы основываются на шифровании с публичными ключами, когда аутентифицирующимся сторонам передаются публичные ключи, с помощью которых и проверяется аутентичность взаимодействующих сторон.

Угрозы безопасности

Требования к безопасности и механизмам превентивной защиты в сфере информационных технологий должны быть адекватны потенциальным угрозам со стороны нарушителя. Данные утверждения верны также и для механизмов аутентификации. Это означает, что при проектировании, разработке и внедрении механизмов аутентификации необходимо принимать во внимание возможные типы атак как на протоколы аутентификации, так и на механизмы их реализации.

Возможные угрозы протоколам аутентификации можно объединить в следующие группы [1-5 и др.]:

1. *Пассивное наблюдение* – является сегодня одной из самых распространенных угроз. Это обусловлено, во-первых, относительной простотой реализации, а во-вторых, сложностью обнаружения со стороны системы безопасности ИС. В случае использования криптографических протоколов аутентификации атака не является действенной, но она может применяться совместно с другими средствами нападения для получения максимально возможного количества информации как об участниках, так и о конкретном протоколе. Шифрование сообщений протокола позволяет обеспечить их конфиденциальность и делает бесполезными действия злоумышленника, если ключи, используемые сторонами, не были скомпрометированы.
2. *Воздействие на обменную информацию*. Это следующая по сложности группа угроз аутентификации. Выражается в том, что злоумышленник перехватывает информацию, видоизменяет ее и отсылает получателю. В итоге получатель уверен, что он аутентифицировался с законным участником протокола, а на самом деле – со злоумышленником. Последствия подобного типа атак могут быть катастрофическими для введенного в заблуждение участника, так как в первую очередь нарушается целостность передаваемой информации. Для приложений, где целостность является главным требованием системы безопасности, нарушение ее и передаваемых сообщений создает соответствующий риск в виде прямых потерь. Именно, исходя из данных соображений, в банковских *информационных* системах обеспечение целостности предаваемых сообщений является приоритетным.
3. *Изменение структуры протокола*. Данный класс злоупотреблений достаточно специфичен и появился в результате анализа криптографических протоколов аутентификации, поскольку атаки первых двух *классов* оказались безрезультатными. Суть данных атак состоит в том, что *злоумышленник* видоизменяет структуру протоколов, после чего законные участники в процессе аутентификации не могут закончить протокол. Последствия могут быть самыми разнообразными – от простого отказа в обслуживании, до получения нарушителем доступа к ресурсам ИС.
4. *Видоизменение механизмов принятия решений*. Данный класс атак не является прямой атакой на протокол, но используется достаточно часто. Он состоит в видоизменении механизмов принятия решений, таких как программы проверки подписи, принятия решений об аутентичности и т.д., особенно привлекательных в случае, когда готовится атака на конкретного участника ИС. Обнаружение подобного рода злоупотреблений возможно только при реализации самозащиты механизмов обеспечения безопасности и наличии доверительной компьютерной базы.

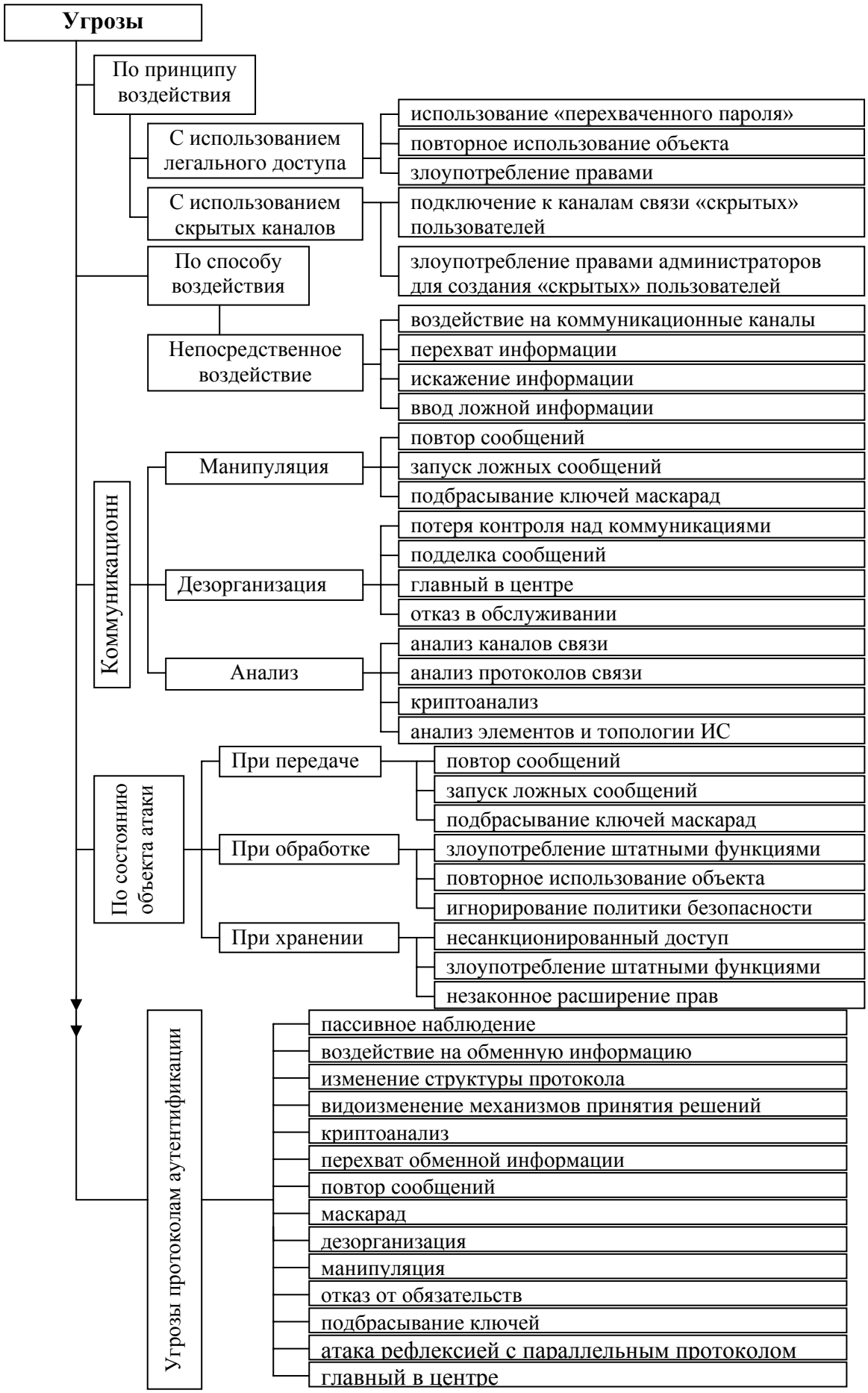

Рис. 2. Классификация угроз безопасности

Рассмотрим наиболее распространенные угрозы процессам аутентификации.

Криптоанализ. Криптоанализ является самым известным методом атаки на любые модели защиты, использующие криптографические операции. Но со становлением криптографии, как отдельной отрасли науки, информационная индустрия пришла к решениям, которые сводят к минимуму усилия криптоаналитика.

Известны атаки на криптографические протоколы без компрометации криптоалгоритма. На практике стратегия криптоаналитика заключается в анализе и разработке атаки на протокол и только в случае неудачи – в атаке криптоалгоритма, что, как правило, требует значительных вычислительных ресурсов и инвестиций. Сегодня большинство пользователей, использующих криптографию для защиты своей информации, выбирают стандартные криптоалгоритмы, прошедшие апробацию, что делает атаку методом криптоанализа на применяемые механизмы практически невозможной.

Перехват обменной информации. Перехват сообщений – это несанкционированное чтение информации. При применении криптографических методов защиты для построения протоколов аутентификации нарушитель не сможет воспользоваться перехваченной информацией, если ему недоступны соответствующие ключи.

Повтор сообщений. Повтор сообщений – это повторная передача ранее регистрированных сообщений. Часто возникает необходимость в том, чтобы получатель был уверен, что моменты формирования, передачи и приема сообщения очень близки друг к другу. Это означает, что отправитель в момент приема сообщения получателем находится на другом конце канала связи. Если получатель не может в этом убедиться, его легко ввести в заблуждение, что зачастую приводит к серьезным последствиям.

Практически данная атака реализуется следующим образом: отправитель формирует и передает сообщение, а нарушитель перехватывает его в канале связи и задерживает до времени, выбираемого по своему усмотрению. Прием устаревшего сообщения в момент, выбранный нарушителем, может быть ненужным или даже представлять опасность для получателя или ИС. Другой способ реализации атаки – перехват, а потом – повтор сообщения. В итоге получатель приходит к выводу, что оно отправлено законным отправителем.

Если при формировании сообщения отправитель применяет защищенную отметку времени, этого достаточно, чтобы исключить возможность задержек, но недостаточно, чтобы защититься от другой опасности – получения сообщения, созданного очень давно.

Практически это может быть реализовано следующим образом. Отправитель или нарушитель под его именем формирует сообщение с будущей отметкой времени и помещает его в электронную почту с инструкцией «передать в указанное время». Отправитель (нарушитель) имеет возможность подготовить целую серию таких сообщений, которые будут поступать получателю в определенные моменты времени, создавая эффект авторского присутствия.

Маскарад. Это попытка выдать себя за другого в целях получения несанкционированного доступа к информационным ресурсам или расширения полномочий. Если строго рассматривать данную угрозу, то на самом деле она означает нарушение состояния аутентификации.

Дезорганизация. Это незаконное изменение адресной части передаваемой информации. Следует отметить, что недооценка данной угрозы может привести к нарушению целостности технологических процессов обработки данных и, соответственно, к значительным материальным потерям. Дезорганизация может привести к *тому*, что кто-то или все не смогут завершить протокол, то есть не смогут аутентифицироваться, а в итоге не получат доступ к информационным ресурсам. Итогом реализации данной угрозы будет отказ в обслуживании.

Манипуляция. Это незаконная замена, вставка, удаление или переупорядочение данных в информационных потоках. В чем-то манипуляция схожа с дезорганизаций. Основное отличие состоит в том, что если дезорганизация не имеет четко сформулированной цели, и последствия могут быть непредсказуемыми, то при манипуляции данными предполагается достижение заранее известной цели.

Отказ от обязательств. Отказ от обязательств – состоит в отказе от ранее принятых или переданных сообщений (взятых на себя обязательств). Данная угроза является самой распространенной в системах электронной торговли и банковских *информационных* системах, когда пользователь отказывается от проведенных ранее транзакций. Развитие технологий, в особенности появление криптографических средств, позволило решить данную проблему.

Применение электронной цифровой подписи позволяет фиксировать авторство сообщения и предупредить отказы от авторства или принятых обязательств.

Подбрасывание ключей. Данная угроза является самой распространенной атакой на протоколы, основанной на криптографии с открытыми ключами. Атака состоит в том, что злоумышленник представляет свой публичный ключ вместо публичного ключа легального пользователя. В случае, если он подписывает сообщение своим секретным ключом, получатель решит, что получил подписанное сообщение от законного участника процесса обмена данными. Эта атака является особо опасной для финансово-банковских систем ввиду того, что злоумышленник может сформировать сообщение от имени законного пользователя, в итоге может быть проведена незаконная транзакция.

Для предотвращения возможности подобного рода атак используется иерархическая система сертификации, реализующая трехсторонние доверительные связи, в результате чего в рамках системы выделяются главные, доверенные органы, которые формируют так называемые сертификаты публичных ключей пользователей. В результате сертификации формируется логическая связь между именем пользователя (держателя ключа) и конкретным публичным ключом. Подпись главного уполномоченного известна всем участникам системы обмена, они могут доверять ей и верить, что публичный ключ, указанный в сертификате, принадлежит пользователю, имя которого значится в этом сертификате.

Атака рефлексией с параллельным протоколом. Состоит в том, что нарушитель начинает встречный протокол. Он (злоумышленник) посылает те же вопросы, которые он получает. Например, если кто-то запрашивает пароль, можно ему же параллельно адресовать это вопрос. В случае получения ответа, его можно вернуть в качестве ответа, и этот ответ будет принят как верный.

Главный в центре. Состоит в том, что нарушитель ведет диалог одновременно с каждым из участников, а они думают, что сообщаются напрямую.

Однозначное отнесение конкретной угрозы к той или иной группе затруднено ввиду их сложности и разносторонности. Но с уверенностью можно определить принадлежность отдельных характеристик угроз к той или иной группе. Более того, с развитием информационных технологий и теории анализа протоколов аутентификации наблюдается появление видов и разновидностей атак, которые совмещают в себе две или более описанных выше угроз. Это означает, что при разработке протоколов аутентификации должны приниматься во внимание их стойкость по отношению не только к обычным угрозам, но и их модификациям и объединению в более сложные, интегрированные.

Большинство протоколов в стандартном исполнении имеют уязвимости и постоянно совершенствуются. Этот процесс предопределяет необходимость проведения исследований, направленных на разработку методологии, в общем, и методик, в частности, в области анализа надежности протоколов, а также построения безопасных протоколов аутентификации.

В теории и практике апробированы комплексы решений, которые можно разделить на два класса:

- модели, использующие логические выводы, в основе которых лежат понятия доверительных отношений;
- методы, ориентированные на построение специализированных атак с применением алгебраических свойств алгоритмов протоколов.

Литература:

1. Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления). //Научно-техническая информация. Серия 1. Организация и методика информационной работы. – 1996, № 5, с.5-13.
2. Черней Г.А., Охрименко С.А., Ляху Ф.С. Безопасность автоматизированных информационных систем. – Кишинев: Ruxanda, 1996. – 186 с.
3. Радев Е., Охрименко С., Черней Г. Информационното противостоене - възможности и оценка на риска. // Автоматика и информатика. София, 2000, № 2-3, с. 14-16.
4. Черней Г.А. Проблемы аутентификации в информационных системах. – Кишинев: Реклама, 2001. – 112 с.
5. Черней Г.А., Охрименко С.А. Анализ на надеждността на протоколите за аутентификация. //Управленски, информационни и маркетингови аспекти на икономическото развитие на балкански страни. София: УНСС, 2004, с.263-277.