УДК 65.011.56

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ЭЛЕКТРОННЫХ УСЛУГ

Горелик С.Л.[1], Ляпер В.С.[1]

[1] *ФГБОУ ВПО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Санкт-Петербург, Россия (197101, г. Санкт-Петербург, Кронверкский проспект, д.49.), e-mail: lyaper@mail.ru*

Проведен анализ проблем информационной безопасности для электронных услуг. Перечислены основные направления развития угроз, среди которых выделена ключевая – угроза безопасности пользовательских атрибутов доступа к электронным услугам. Произведено сравнение существующих подходов для обеспечения безопасности пользовательских атрибутов доступа к электронным услугам, выявлены недостатки существующих решений, связанные с низким уровнем безопасности и структурой пользовательского интерфейса. Обоснована актуальность повышения уровня информационной безопасности для услуг банковского сектора, электронной коммерции и государственных электронных услуг. Предложено решение в виде программно-аппаратного комплекса, выполняющего функции управления пользовательскими атрибутами доступа на базе облачных технологий, позволяющего повысить уровень информационной безопасности и эргономики при доступе к электронным услугам.

Ключевые слова: информационная безопасность, облачные услуги, электронная коммерция.

ELECTRONIC SERVICES INFORMATION SECURITY ISSUES OVERVIEW

Gorelik S.L.[1], Lyaper V.S.[1]

[1] *St-Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint-Petersburg, Russia (197101, Saint-Petersburg, Kronverkskiy pr., 49), e-mail: lyaper@mail.ru*

The review of the information security issues for e-services is presented. Main trends were taken into account, among them key threat was identified – user identity and credentials security. Technical approaches for credentials protection were compared, as a result revealed the shortcomings of existing solutions associated with a low level of safety and user interface. The urgency of increasing the level of information security services for banking, e-commerce and e-government services was illustrated. Proposed solution in the form of hardware and software to perform the functions for managing user identity and credentials based on cloud technology to increase the level of information security and ergonomics for access to electronic services.

Keywords: information security, cloud services, e-commerce.

Информационная безопасность становится ключевым фактором в процессе предоставления электронных услуг. Современные инфокоммуникационные услуги отличаются использованием большого объема чувствительной информации, которая нуждается в защите (персональные данные, платежная информация, ключи и секреты).

Можно выделить ключевые элементы, безопасность которых критически важна для предоставления услуг в электронном виде (серверное оборудование и приложения, включая облачные структуры, каналы связи, пользовательское оборудование и приложения, ключи и идентификаторы). Безопасность на стороне серверов приложений, каналов связи и пользовательского оборудования и ПО достаточно хорошо изучена [7, 8, 9, 10]. Но проблема безопасности при пользовании ключами и идентификаторами решается, в основном, на уровне практических приложений и опыта, что явно недостаточно, с точки зрения количественной оценки уровней защищённости на стадиях проектирования и создания

оптимальных пользовательских интерфейсов. Научный анализ указанной проблемы является предметом настоящей работы.

Материал и методы исследования

Среди наиболее часто эксплуатируемых угроз информационной безопасности называется эксплуатация уязвимостей протоколов аутентификации и управления сессиями пользователей [6]. Данный вид угроз информационной безопасности занимает вторую строчку рейтинга, сразу после встраивания вредоносного кода, которое нередко производится силами злоумышленников-инсайдеров, и направлено на хищение атрибутов доступа пользователя. Доля рисков информационной безопасности, связанных с атрибутами доступа пользователей, неуклонно возрастает – в 2010 году эта угроза занимала третье место в рейтинге OWASP [12].

Имеются оценки экономического ущерба, который приносит компрометация пользовательских атрибутов доступа: по данным анализа базы данных инцидентов ИБ WHID наибольшую долю от всех действий злоумышленников составляют финансовые потери (64%), при этом в 36% случаев **использовались украденные или скомпрометированные пароли и другие атрибуты доступа** [13]. В сфере розничной торговли наибольшие потери были понесены (в 27% посягательств злоумышленников) из-за компрометации информации о кредитных картах, т.е. фактически данных об **идентификаторах покупателей [13]**.

Анализ

Можно утверждать, что обеспечение безопасности ключей пользователя (атрибутов доступа к электронным услугам, паролей, идентификаторов и т.п.) на сегодняшний день наиболее актуально. В действительности, положение вещей обстоит следующим образом: провайдеры электронных услуг предпочитают снимать с себя любую ответственность, касающуюся защиты атрибутов доступа пользователей, внося соответствующие пункты в пользовательское соглашение. Пользователь сам обязан обеспечивать безопасность своих ключей. При этом если средств и способов защиты оборудования, ПО и информации на стороне провайдера на рынке имеется в достаточном количестве, то защита ключей пользователей находится в зачаточном состоянии, несмотря на актуальность этого вопроса. В то время как для защиты каналов связи, серверного ПО и оборудования используются сложные комплексы административно-технических средств, разработаны методики оценки уровня ИБ и рисков, в т.ч. на уровне государств [11], рекомендации для пользователей по управлению паролями сводятся, практически, к предупредительному информированию («Держите свои пароли в тайне, их компрометация может привести к серьезной угрозе информационной безопасности»).

С другой стороны, защищенный жизненный цикл ключей и идентификаторов на сегодняшний день становится все более существенным фактором в безопасности электронных услуг. Чтобы сместить акценты безопасности ключей и идентификаторов со стороны пользовательских рисков, повысить уровень их ИБ и ИБ электронных услуг в целом, необходимо реализовать ряд мероприятий и технических мер:

– обеспечить защищенную генерацию ключей и идентификаторов;

– обеспечить защищенное хранение и использование ключей и идентификаторов;

– разработать универсальные механизмы использования ключей в различного рода электронных услугах;

– реализовать сопутствующие механизмы авторизации и управления доступом;

– разработать методики оценки уровня ИБ и рисков при использовании различных комбинаций ключей и идентификаторов и на основе них выбрать оптимальные способы доступа для отдельных видов электронных услуг.

Комплекс перечисленных выше мероприятий по управлению жизненным циклом ключей и идентификаторов образует набор механизмов управление доступом и его атрибутами (I&AM).

Современная парадигма механизмов I&AM представляет собой многоуровневую структуру, реализуемую посредством комплекса административно-технических мероприятий:

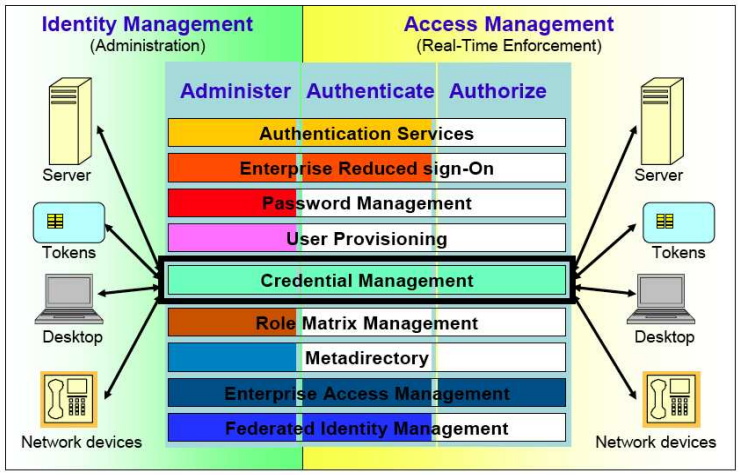

Рис. 1. Структура средств I&AM

Управление доступом и пользовательскими атрибутами позволяет решать задачи по обеспечению безопасности доступа к гетерогенным электронным услугам:

— защищать пользовательские пароли, идентификаторы и другие атрибуты доступа;

— управлять пользователями и уровнями авторизации пользователей;

— выстраивать единые политики безопасности для приложений различного уровня сложности (на уровне организации или государства);

— предоставлять средства безопасности как сервис.

Одна из важнейших задач, решаемых средствами I&AM, – обеспечение безопасности самих атрибутов доступа (паролей, секретов, идентификаторов и т.п.) и их безопасное использование. Данная функция может реализовываться различными методами, например:

— использованием специальных технических средств для защиты ключей и идентификаторов (одним из вариантов являются токены и смарт-карты);

— использованием облачных средств защиты информации, таким образом, чаще всего реализуются функции управления паролями (Password Management);

— комбинированные механизмы, сочетающие в себе персональные носители и облачные услуги.

В таблице 1 проведено сравнение методов защиты ключей и идентификаторов для обеспечения безопасности пользовательских атрибутов доступа к электронным услугам.

Таблица 1

Критерий	**Токены, смарт-карты**	**Облачные услуги**	**Комбинированные средства защиты ключей**
Форм-фактор	Персональный защищенный носитель данных	Защищенная облачная услуга	Комбинации в виде облачного хранилища ключей с доступом посредством персонального защищенного носителя данных
Совместимые платформы	Требуется наличие специальных устройств-считывателей, плохо распространены на мобильных устройствах	Все программно-аппаратные платформы	Все программно-аппаратные платформы
Типы услуг, к которым предоставляется доступ	Онлайн и оффлайн услуги	Только онлайн услуги	Онлайн и оффлайн услуги
Уровень информационной безопасности при аутентификации	Высокий	Определяется способом аутентификации при доступе к облаку, обычно ниже, чем у токенов	Определяется способом аутентификации при доступе к облаку, за счет использования физического носителя секрета может быть высоким

Необходимость наличия специализированного ПО	Необходимо СПО	СПО не требуется	В зависимости от уровня ИБ, может дополнительно применяться СПО
Требования по аппаратной совместимости	Наличие считывателя	Не предъявляются	В общем случае не предъявляются
Возможность защиты идентификаторов	Не предусмотрена, но может быть реализована	Присутствует	Присутствует
Привязка ключей и идентификаторов к личности пользователя	Есть	В общем случае нет	Есть
Удобство использования со стороны пользователей	Удобство пользования ограничено требованием наличия считывателя и СПО	Удобство на уровне обычной интернет-услуги	Удобство на уровне обычной интернет-услуги

Из приведенной таблицы следует, что наиболее универсальным средством защиты ключей и идентификаторов является комбинированный вариант, совмещающий в себе удобство облачного хранилища и безопасность персонального защищенного носителя информации. Проблема управления множественными пользовательскими атрибутами доступа, ключами и идентификаторами крайне остро стоит в настоящее время перед предприятиями финансовой отрасли и банками. Участились случаи мошенничества, связанные с попытками получить доступ к ключам пользователей (PIN-коды, коды телефонной аутентификации), одноразовым паролям и TAN [4] и самим номерам кредитных карт [2]. Банки традиционно возлагают ответственность за безопасность платежных и кредитных карт на клиента, однако злоумышленнику достаточно знать только номер карты, чтобы совершить перевод денег с нее [3]. В настоящее время банки находятся в поиске эффективных решений, позволяющих повысить безопасность средств доступа, используемых для услуг ДБО.

Торговые организации, в отличие от, например, банков, не всегда имеют достаточно развитую сеть, а с развитием интернет-коммерции у многих компаний её вообще нет, чтобы обрабатывать первичную регистрацию клиентов. В то же время для осуществления ряда коммерческих сделок необходимо привязывать атрибуты доступа пользователя к электронной услуге к личности пользователя. Это становится особенно актуальным в связи с переводом договорных отношений в электронную форму.

Для государственного сектора в соответствии с распоряжением правительства от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)» будет проведена работа по переводу

государственных и муниципальных услуг в электронную форму. На сегодняшний день уже реализована ЕСИА, разработаны решения по персональным атрибутам доступа для граждан (токены с ЭЦП, пароли, УЭК). Однако количество пользователей, предпочитающих защищенные средства доступа к госуслугам, по-прежнему невелико. Так, например, УЭК выдано по самым оптимистичным подсчетам около 100 тыс. [5], а токенов с ЭЦП по некоторым оценкам выпущено ещё меньше. Главный недостаток средств доступа к госуслугам – удобство использования – вызван форм-фактором устройства защиты ключей в виде персонального носителя.

Из всего перечисленного выше можно сделать вывод о том, что задачи управления пользовательскими атрибутами доступа I&AM на сегодняшний день решены в недостаточном объеме и требуется кардинальный пересмотр подхода к обеспечению безопасности пользовательских атрибутов доступа.

Реализация и выводы

Наиболее подходящим решением задачи обеспечения управления пользовательскими атрибутами доступа для гетерогенных электронных услуг является решение на базе комбинированного подхода, сочетающего в себе привычные, с высоким уровнем безопасности, персональные носители и облачные хранилища ключей. Персональный носитель может обеспечивать лишь доступ пользователя к облаку, решающему основные задачи по управлению ключами и идентификаторами.

Предлагаемое решение должно соответствовать количественным параметрам, на основании которых можно будет оценить, насколько полно оно решает поставленную задачу:

— надежность (оценивается вероятностью безотказной работы в течение определенного периода времени, рассчитанного с учетом стоимости для пользователя каждого отказа);

— уровень информационной безопасности (способность системы обеспечивать конфиденциальность, целостность и доступность ключей и идентификаторов пользователей);

— устойчивость (способность системы сохранять свою работоспособность при внешних, в т.ч. вредоносных воздействиях);

— эргономичнсоть (userabiliry) (удобство использования средств системы в различных электронных услугах);

— стоимость.

Указанные параметры для целевого решения должны быть выше, чем для уже существующих подходов обеспечения безопасности ключей, идентификаторов и пользовательских атрибутов доступа в целом [1].

С учетом перечисленного выше, задача, которая обеспечивает достижение необходимого уровня значений параметров в системах управления пользовательскими атрибутами доступа, формулируется как разработка механизмов управления пользовательскими атрибутами доступа, обеспечивающих:

— массовый, недорогой, защищенный доступ к гетерогенным электронным услугам;

— пригодность для использования в различных прикладных областях, в т.ч. в электронной коммерции, дистанционном банковском обслуживании и государственных электронных услугах.

Для решения сформулированной задачи разработана комбинированная система управления пользовательскими атрибутами доступа к электронным услугам, выполняющая следующие функции:

— облачное хранение пользовательских паролей, идентификаторов и других атрибутов доступа;

— доступ к облачному хранилищу посредством физического защищенного носителя, на базе двухфакторной схемы аутентификации, например, по связке мобильный телефон (или токен) и мастер-пароль;

— использование в решении процедур регистрации пользователей, предполагающих привязку профиля пользователя, а следовательно, и всех ключей и идентификаторов, к личности пользователя;

— предоставление набора услуг информационной безопасности для внешних систем (аутентификация, авторизация, управление паролями и т.п.);

— наличие интерфейсов для взаимодействия с целевыми потребителями услуг.

Система реализована в формате аппаратно-программного комплекса, в основе которого лежат облачные технологии распределенного хранения информации. За счет использования облачного подхода для хранения и защиты ключей и идентификаторов пользователей повышается надежность и устойчивость системы в целом. Функционально система выглядит следующим образом:

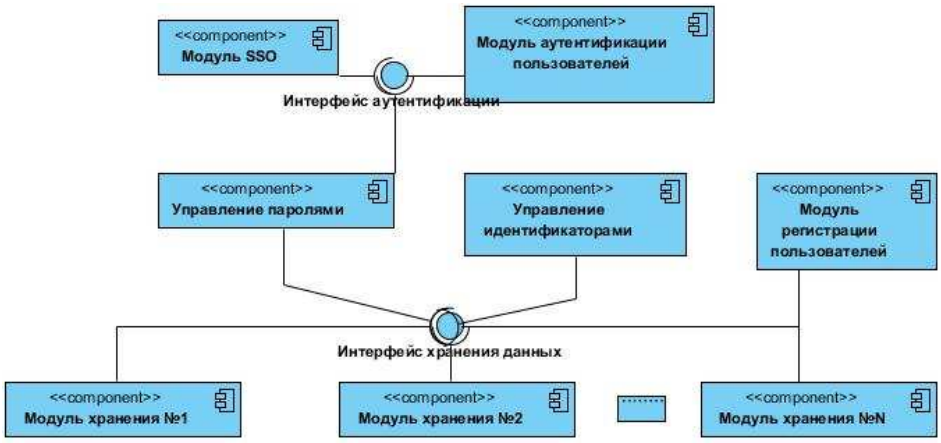

Рис. 2. Функциональная схема решения

Система реализована в виде взаимосвязанных модулей, каждый из которых реализует набор функций по управлению пользовательскими атрибутами доступа: модульрегистрации пользователей производит обработку регистрационных запросов, их верификацию и сохранение в системе, хранение данных реализовано в виде распределенного облачного модуля хранения, состоящего из N-компонент, аутентификация пользователей выполняется соответствующим модулем, помимо этого присутствуют модули для реализации доступа с помощью паролей, а также системы SSO и модуль управления идентификаторами, реализующий их защищенное использование в электронных услугах.

Значения параметров характеристики надежности, устойчивости, информационной безопасности, удобства и стоимости предлагаемого решения для целевых приложений, рассмотренных в настоящей работе выше, чем у имеющихся на настоящий момент общих решений аналогичного класса. Оценка соответствия указанным характеристикам может быть произведена в соответствии с стандартными методологиями оценки ИБ [1, 7, 8, 9, 10].

Сокращения и аббревиатуры

ДБО – дистанционное банковское обслуживание.

ЭЦП – электронная цифровая подпись.

УЭК – универсальная электронная карта.

ЕСИА – единая система идентификации и аутентификации для портала государственных услуг.

ИБ – информационная безопасность.

ПО – программное обеспечение.

СПО – специализированное программное обеспечение.

I&AM – Identity and Access Management (I&AM).

OWASP – Open Web Application Security Project.

SSO – Single-Sign-On.

TAN – transaction authorization number.

WHID – Web Hacking Incidents Database.

Список литературы

1. Липаев В.В. Надежность программных средств. – М.: Синтег, 1998. – 232 с.
2. Мегафон – Мобильное мошенничество в сфере дистанционного банковского обслуживания [Электронный ресурс]. — Режим доступа: http://ru-megafon.livejournal.com/216017.html (дата обращения: 01.08.2013).
3. Мошенничество с использованием пластиковых карт / Хабрахабр [Электронный ресурс]. — Режим доступа: http://habrahabr.ru/post/109361/ (дата обращения: 01.08.2013).
4. Обнаружена программа, предоставляющая незаконный доступ к счетам [Электронный ресурс]. — Режим доступа: http://www.plusworld.ru/daily/obnarujena-programma-pohischauschaya-kluchi-u-polzovateley-internet-bankinga-cherez-sms/ (дата обращения: 01.08.2013).
5. CNews: Универсальная электронная карта [Электронный ресурс]. — Режим доступа: http://uec.cnews.ru/reviews/index.shtml?2013/07/28/536874 (дата обращения: 01.08.2013).
6. Category: OWASP Top Ten Project – OWASP [Электронный ресурс] – URL: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013 (дата обращения: 01.08.2013).
7. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. August 1999. Version 2.1 CCIMB-99-031.
8. Common Criteria for Information Technology Security Evaluation Part 2 : Security functional requirements Version 2.0 May 1998 CCIB-98-027.
9. Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance requirements Version 2.0 May 1998 CCIB-98-028125.
10. Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology. Version 1.0 August 1999 CEM-99/045.
11. Cichonski P., Millar T., Grance T., Scarfone K. NIST Special Publication 800-61 Revision 2, Computer Security Incidents Handling Guide URL: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf (дата обращения: 01.08.2013).
12. Top 10 2010-Main – OWASP [Электронный ресурс] – URL: https://www.owasp.org/index.php/Top_10_2010-Main (дата обращения: 01.08.2013).

13. Web Application Security | Web Hacking | Trustwave [Электронный ресурс] – URL: https://www.trustwave.com/trustednews/2011/03/web-hacking-incident-database-report-reveals-increase-in-ddos-attacks#sthash.5lvLg2KW.dyz2zauj.dpbs (дата обращения: 01.08.2013).

Рецензенты:

Тарлыков В.А., д.т.н., профессор, начальник управления проектирования образовательных программ федерального государственнго бюджетнго образовательнго учереждения высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург.

Стафеев С.К., д.т.н., профессор, заведующий кафедрой «Университета ИТМО», г. Санкт-Петербург.