Алексей Игоревич Александров, Евгений Александрович Роганов
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, г. Москва, 115409, Россия
e-mail: aialeksandrov@mephi.ru, ORCID 0000-0001-7868-165X;
e-mail: earoganov@mephi.ru,ORCID 0000-0001-8207-2179

МОДИФИКАЦИЯ CAS-ПРОТОКОЛА ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DOI: http://dx.doi.org/10.26583/bit.2017.3.05

Аннотация. Распространение информационных технологий, а также расширение сфер их применения требуют от разработчиков программного обеспечения постоянного повышения уровня безопасности при работе пользователей с конфиденциальной информацией и персональными данными. Задача организации безопасной аутентификации пользователей в информационных системах является, пожалуй, одно из самых распространенных проблем, которые возникают при разработке практически любого программного обеспечения. Несмотря на наличие огромного существующего на сегодняшний день количества средств аутентификации, регулярно появляются новые способы, механизмы и технологии организации данного процесса, повышающие, в первую очередь, уровень защиты данных от несанкционированного доступа к ним. В данной статье рассматривается опыт применения централизованной системы аутентификации пользователей на основе CAS-протокола (CAS - Central Authentication Service, служба централизованной аутентификации) и свободно распространяемого программного обеспечения с открытым исходным кодом. В рамках работы проанализированы его основные преимущества и недостатки, а также рассмотрены возможности его модификации с целью повышения уровня защиты веб-ориентированных информационных систем от несанкционированного доступа. Рассмотрены механизмы, позволяющие установить максимальную продолжительность непрерывной работы в сервисах, использующих централизованную систему аутентификации, а также рассмотрены проблемы применения современных веб-технологий при использовании системы аутентификации, базирующейся на CAS-протоколе. В статье рассмотрены возможности модернизации CAS-сервера с целью реализации дополнительных модулей: модуль сбора и анализа статистики использования информационных систем, система управления пользователями, а также рассмотрены особенности его применения в образовательной организации с целью формирования единой информационно-образовательной среды.

Ключевые слова: безопасность веб-приложений, CAS-протокол, централизованная система аутентификации, CAS, аутентификация пользователей, Ruby on Rails.

Для цитирования. **АЛЕКСАНДРОВ, Алексей Игоревич; РОГАНОВ, Евгений Александрович.** МОДИФИКАЦИЯ CAS-ПРОТОКОЛА ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 43-49, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/263>. Дата доступа: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.05.

Alexey Igorevich Alexandrov, Eugene Alexandrovich Roganov
National Research Nuclear University MEPhI,
Kashirskoe shosse, 31 Moscow, 115409, Russia
e-mail: aialeksandrov@mephi.ru, ORCID 0000-0001-7868-165X;
e-mail: earoganov@mephi.ru, ORCID 0000-0001-8207-2179

Modification of CAS-protocol for improvement of security web-applications from unauthorized access

DOI: http://dx.doi.org/10.26583/bit.2017.3.05

Abstract. Dissemination of information technologies and the expansion of their application demand constantly increasing security level for users, operating with confidential information and personal data. The problem of setting up secure user identification is probably one of the most common tasks, which occur in the process of software development. Today, despite the availability of a large amount of authentication tools, new solutions, mechanisms and technologies are being introduced regularly. Primarily, it is done to increase the security level of data protection against unauthorized access. This article describes the experience of using central user authentication service based on CAS-protocol (CAS – Central Authentication Service) and free open source software, analyzing its main advantages and disadvantages and describing the possibility of its modification, which would increase security of web-based information systems from being accessed illegally. The article contains recommendations for setting a maximum time limit for users working on services, integrated with central authentication; and, analyses the research of implementing modern web-technologies while using user authentication system based on CAS-protocol. In addition, it describes the ways of CAS-server modernization for developing additional modules: a module for collecting and analyzing the use of information systems, and another one, for a user management system. Furthermore, CAS-protocol can be used at universities and other organizations for creating a unified information environment in education.

Keywords: web application security, CAS-protocol, central authentication service, CAS, user authentication, Ruby on Rails.

For citation. **ALEXANDROV, Alexey I Igorevich; ROGANOV, Eugene Alexandrovich.** Modification of CAS-protocol for improvement of security web-applications from unauthorized access. IT Security, [S.l.], v. 24, n. 3, p. 43-49, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/263>. Date accessed: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.05.

Введение

Современное масштабное развитие информационных технологий с каждым годом повышает требования к безопасности использования информационных систем, а также защите персональных данных от несанкционированного доступа к ним. На сегодняшний день в качестве одного из основных средств идентификации пользователя используются аутентификация пользователя с помощью входного имени (логина) и пароля.

На сегодняшний день человеку, активно использующему информационные технологии, ежедневно приходится сталкиваться с огромным числом различных систем, сервисов и служб, каждая из которых, как правило, требует для своего использования предварительной регистрации и аутентификации с использованием логина и пароля [1]. Значительная доля пользователей использует одинаковое имя пользователя и пароль на различных сервисах, что создает угрозу несанкционированного доступа к ресурсам информационных систем, хранящих, в том числе, и персональные данные пользователей.

Функционирование современного высшего учебного заведения трудно представить без информационных технологий. В Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ) используется целый ряд различных информационных систем, в работу с которыми включены все участники деятельности вуза: преподаватели, студенты, аспиранты, абитуриенты, слушатели подготовительного отделения, администрация Университета и ряд других. Наличие в НИЯУ МИФИ значительного количества обособленных структурных подразделений обуславливает необходимость широкого применения информационных технологий, а также современных и надежных

инструментов для защиты данных от несанкционированного доступа. Большое количество информационных систем, используемых государственными учреждениями, так или иначе, включают в себя средства межсистемной аутентификации и идентификации [2]. Таким образом, создание централизованной системы аутентификации и ее внедрение в рамках образовательного учреждения с большим количеством обособленных структурных подразделений является актуальной задачей [3,4].

CAS-сервер как средство аутентификации

Многие информационные системы, используемые в МИФИ, являются веб-ориентированными системами, а для аутентификации пользователей используется пара логин-пароль. С целью создания единого информационного пространства, а также с целью формирования единой информационно-образовательной среды в НИЯУ МИФИ было принято решение использовать в качестве средства аутентификации пользователей модифицированную версию CAS-протокола [5] (CAS[6] — Central Authentication Service, служба централизованной аутентификации), определяющего порядок взаимодействия CAS-сервера, пользователей и веб-приложений, являющихся CAS-клиентами. CAS-сервер, по сути, является единой точкой входа во все ресурсы информационной среды. Общая схема аутентификации пользователя на основе CAS-протокола приведена на рис. 1. Применение данной технологии позволяет повысить удобство использования информационных систем для конечного пользователя, избавив его от необходимости многократного ввода имени пользователя и пароля в различных информационных системах и сервисах организации [7], а также повысить безопасность единой информационной среды, обеспечив централизованное хранение информации об учетных данных пользователя, ограничив внешние информационные системы от необходимости передачи и хранения конфиденциальных данных, используемых для аутентификации.

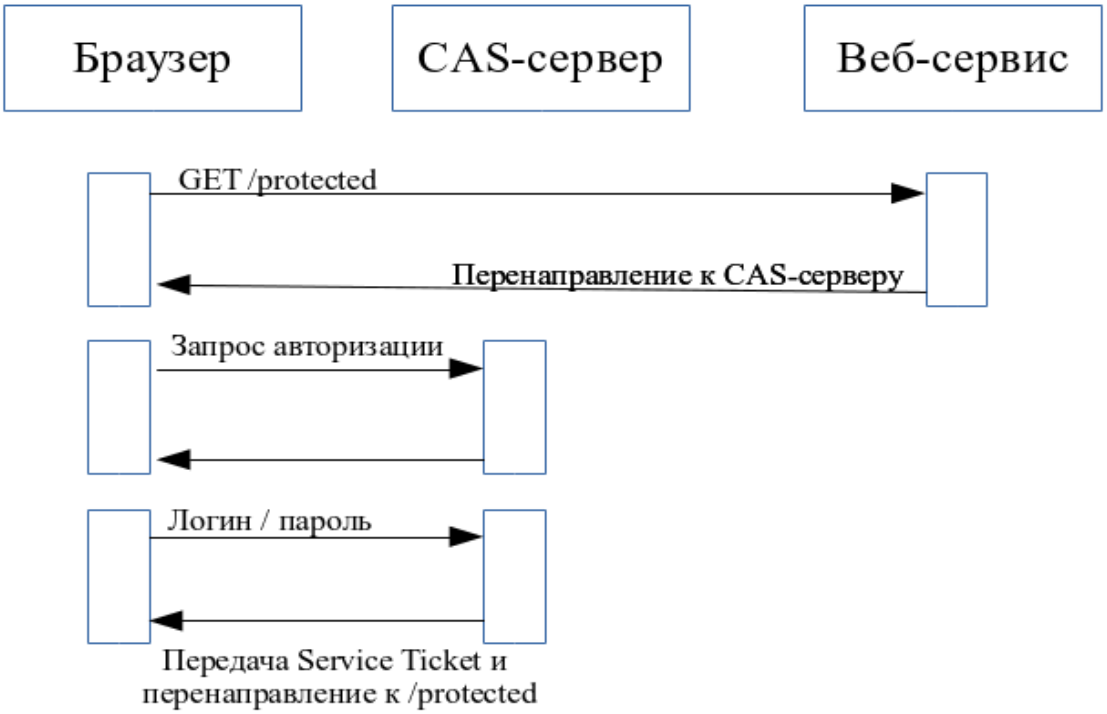

Рисунок 1 - Схема аутентификации на основе CAS-протокола
(Fig. 1 - Authentication scheme based on the CAS Protocol)

На данный момент существует несколько реализаций CAS-сервера: Apereo CAS [8], Ruby CAS [9] и ряд других, использующие различные языки программирования, но имеющих схожие идеи реализации. Большинство разрабатываемых в Управлении информационно-методического обеспечения образовательного процесса НИЯУ МИФИ веб-приложений функционируют на основе свободно распространяемой среды с открытым исходным кодом Ruby on Rails [10], которая предоставляет разработчикам инструменты для быстрого создания современных веб-приложений. По этой причине в качестве основы для реализации адаптированной для НИЯУ МИФИ версии CAS-сервера был выбран CASino [11], реализованный на основе языка программирования Ruby [12]. Среди преимуществ данного продукта можно отметить возможность его интеграции с другими системами аутентификации, двухфакторной авторизации, а также локализации для нескольких языков.

Мировой опыт использования центрального сервера аутентификации, а также широкое применение технологий AJAX (Asynchronous Javascript and XML), WebSocket, Turbolinks и ряда других побуждают к внесению изменений в «канонический» CAS-протокол.

При использовании классического CAS-протокола пользователю после успешной аутентификации выдается специальный уникальный в единицу времени ключ — Ticket Granting Ticket, позволяющую получить Service Ticket для работы с внешним веб-сервисом. Веб-приложение после получения Service Ticket более не обязано обмениваться запросами с CAS-сервером, считая пользователя успешно прошедшим аутентификацию и позволяя ему работать в системе бесконечно долго. Возможность работы с другими веб-приложениями без повторного ввода имени пользователя и паролем обеспечивается наличием Ticket Granting Ticket, имеющим определяемый CAS-сервером срок действия.

В модифицированной нами версии CAS-протокола используется иная политика проверки выданных CAS-серверов «билетов» (tickets). Каждый из CAS-клиентов периодически обмениваются информацией с CAS-сервером для сигнализирования об активности пользователя в системе. Это позволяет, в первую очередь, принять решение о продлении срока действия Ticket Granting Ticket, а во-вторых получить данные для сбора статистики и анализа работы пользователей в информационных системах. Подобное изменение позволяет также задать максимальное время бездействия пользователя в системе, по истечении которого завершается действие выданного билета, что означает для конечного пользователя необходимость прохождения повторной аутентификации. Данная процедура позволяет значительно повысить защиту информационных систем от несанкционированного доступа третьих лиц, особенно в случаях использования одной и той же учетной записи браузера различными пользователями, а также избежать приема и передачи паролей внешним сервисам и информационным системам.

Дополнительные модули CAS-сервера

В рамках работы по модернизации CAS-протокола дополнительно был реализован модуль, обеспечивающий получение статистики доступа к CAS-серверу пользователями различных информационных систем, его использующих. Пример интерфейса данного модуля представлен на рис. 2.

Модуль статистики позволяет получить информацию не только о действиях пользователя в информационных системах, применяющих для аутентификации CAS-сервер, но и информацию о дате, времени, IP-адресе и версии браузера, под которыми эти действия выполнялись. Сбор и хранение подобной информации позволяет реализовать систему аналитики и визуализации для принятия решений об эффективности

функционирования и повышает удобство использования различных информационных систем [13].

С целью реализации системы управления пользователями CAS-сервера выполнена его интеграция с Корпоративным порталом НИЯУ МИФИ [14]. В результате проделанной работы удалось объединить информацию о пользователях Корпоративного портала и пользователях CAS-сервера, что, в свою очередь, позволило реализовать интерфейсы изменения пароля пользователями, а также обеспечить возможность восстановления забытого пароля с помощью адреса электронной почты, привязанного к учетной записи пользователя CAS-сервера.

https://home.mephi.ru/home	24 марта 2017, 05:53	24 марта 2017, 05:53	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0	85.143.112.47
https://staff.mephi.ru/people/search_index	23 марта 2017, 14:31	23 марта 2017, 14:31	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0	127.0.0.1
https://home.mephi.ru/vote_deps?page=2	23 марта 2017, 13:12	23 марта 2017, 13:12	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0	127.0.0.1
https://home.mephi.ru/bookmarks	23 марта 2017, 11:56	23 марта 2017, 11:56	Mozilla/5.0 (Linux; Android 6.0.1; MI NOTE LTE Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Mobile Safari/537.36	85.143.112.41

Рисунок 2 - Интерфейс просмотра статистики пользователя
(Fig. 2 - The statistics interface user)

Заключение

В результате анализа канонического CAS-протокола удалось выявить его основные недостатки, внести изменения в CAS-протокол, тем самым повысив безопасность его использования как основного средства аутентификации пользователя. В рамках работы реализованы модифицированные версии CAS-сервера и CAS-клиента, позволяющие организовать централизованную аутентификацию пользователей в информационных системах НИЯУ МИФИ [15]. CAS-сервер является неотъемлемой частью единого информационного пространство университета. Реализованные дополнительные модули позволили значительно расширить функционал и возможности системы управления пользователями, а также получить инструменты сбора и анализа информации о работе пользователей в информационных системах университета. Система реализована и функционирует на основе свободного программного обеспечения с открытым исходным кодом.

СПИСОК ЛИТЕРАТУРЫ:

1 П.П. Кейно. Иерархическая модель прав доступа в декларативном языке моделирования веб-приложений по методолгии BlockSet. Безопасность информационных технологий. 2016. №1. С. 53-58.
2 М.В. Ванин, И.А. Трифаленков, В.И. Королев. Единая система идентификации и аутентификации как национальный сервис инфраструктуры электронного правительства. Безопасность информационных технологий. 2013. №1. С. 39-42.
3 Alexov, A.; Deighton, D.; Doggett, J.; McCuen, L.; Russell, R.; Yermolaev, A. C hoosing a Single Sign-On Solution at STScI. Astronomical Data Analysis Software and Systems XXIII. Proceedings of a meeting held 29 September - 3 October 2013 at Waikoloa Beach Marriott, Hawaii, USA. Edited by N. Manset and P. Forshay ASP conference series, vol. 485, 2014, p.289.
4 Brachmann, Eric, Dittmann, Gero, Schubert, Klaus-Dieter. Simplified Authentication and Authorization for RESTful Services in Trusted Environments – Berlin; Heidelberg: Springer-Verlag, 2012. p. 244-258.
5 CAS-protocol. [Электронный ресурс]. URL: https://apereo.github.io/cas/4.2.x/protocol/CAS-Protocol.html (дата обращения 24.03.2017).
6 Central Authentication Service. [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Central_Authentication_Service (дата обращения 24.03.2017).
7 Suoranta S., Heikkinen J., Silvekoski P. (2012) Authentication Session Migration. In: Aura T., Järvinen K., Nyberg K. (eds) Information Security Technology for Applications. NordSec 2010. Lecture Notes in Computer Science, vol 7127. Springer, Berlin, Heidelberg
8 Apereo CAS - Enterprise Single Sign On for all earthlings and beyond. [Электронный ресурс]. URL: https://github.com/apereo/cas (дата обращения 24.03.2017).
9 Provides single sign-on authentication for web applications, implementing the server-end of Jasig's CAS protocol. [Электронный ресурс]. URL: https://github.com/rubycas/rubycas-server (дата обращения 24.03.2017).
10 Ruby on Rails - A web-application framework that includes everything needed to create database-backed web applications according to the Model-View-Controller (MVC) pattern. [Электронный ресурс]. URL: http://rubyonrails.org/ (дата обращения 05.04.2017)
11 CASino. [Электронный ресурс]. URL: http://casino.rbcas.com/ (дата обращения 24.03.2017).
12 Язык программирование Ruby. [Электронный ресурс]. URL: https://www.ruby-lang.org (дата обращения 24.03.2017).
13 Z.A. Pardos, A. Whyte, K. Kao. moocRP: Enabling Open Learning Analytics with an Open Source Platform for Data Distribution, Analysis, and Visualization. Technology, Knowledge and Learning, 2016. vol. 21. Issue 1. pp. 75-98. doi: 10.1007/s10758-015-9268-2
14 Корпоративный портал НИЯУ МИФИ. [Электронный ресурс]. URL: https://home.mephi.ru (дата обращения 24.03.2017).
15 Служба централизованной аутентификации НИЯУ МИФИ. [Электронный ресурс]. URL: https://auth.mephi.ru (дата обращения 24.03.2017).

REFERENCES:

[1]P.P. Keyno. Hierarchical Permissions Model in the Declarative Web-Application Modeling Language in Context of BlockSet Metodology. Bezopasnost’ informacionnyh tehnologij (IT Security). 2016. no 1. pp. 53-58. (in Russian)
[2]M.V. Vanin, I.A. Trifalenkov, V.I. Korolev. Single identification and authentication system as national service of infrastructure for electronic government. Bezopasnost’ informacionnyh tehnologij (IT Security). 2013. no 1. pp. 39-42. (in Russian)

[3]Alexov, A.; Deighton, D.; Doggett, J.; McCuen, L.; Russell, R.; Yermolaev, A. C hoosing a Single Sign-On Solution at STScI. Astronomical Data Analysis Software and Systems XXIII. Proceedings of a meeting held 29 September - 3 October 2013 at Waikoloa Beach Marriott, Hawaii, USA. Edited by N. Manset and P. Forshay ASP conference series, vol. 485, 2014, p.289.
[4]Brachmann, Eric, Dittmann, Gero, Schubert, Klaus-Dieter. Simplified Authentication and Authorization for RESTful Services in Trusted Environments – Berlin; Heidelberg: Springer-Verlag, 2012. p. 244-258.
[5]CAS-protocol. URL: https://apereo.github.io/cas/4.2.x/protocol/CAS-Protocol.html (access date 2017/03/24).
[6]Central Authentication Service. URL: https://en.wikipedia.org/wiki/Central_Authentication_Service (access date 2017/03/24).
[7]Suoranta S., Heikkinen J., Silvekoski P. (2012) Authentication Session Migration. In: Aura T., Järvinen K., Nyberg K. (eds) Information Security Technology for Applications. NordSec 2010. Lecture Notes in Computer Science, vol 7127. Springer, Berlin, Heidelberg
[8]Apereo CAS - Enterprise Single Sign On for all earthlings and beyond. URL: https://github.com/apereo/cas (access date 2017/03/24).
[9]Provides single sign-on authentication for web applications, implementing the server-end of Jasig's CAS protocol. URL: https://github.com/rubycas/rubycas-server (access date 2017/03/24).
[10] Ruby on Rails - A web-application framework that includes everything needed to create database-backed web applications according to the Model-View-Controller (MVC) pattern. URL: http://rubyonrails.org/ (access date 2017/04/05).
[11] CASino. URL: http://casino.rbcas.com/ (access date 2017/03/24).
[12] Ruby Programming Language. URL: https://www.ruby-lang.org/ (access date 2017/04/05).
[13] Z.A. Pardos, A. Whyte, K. Kao. moocRP: Enabling Open Learning Analytics with an Open Source Platform for Data Distribution, Analysis, and Visualization. Technology, Knowledge and Learning, 2016. vol. 21. Issue 1. pp. 75-98. doi: 10.1007/s10758-015-9268-2
[14] Corporate system of MEPhI. URL: https://home.mephi.ru (access date 2017/03/24).
[15] Central Authentication Service of MEPhI. URL: https://auth.mephi.ru (access date 2017/03/24).