DOI 10.37882/2223–2966.2022.10.15

МЕТОДИКА СРАВНЕНИЯ СОВРЕМЕННЫХ МЕТОДОВ АУТЕНТИФИКАЦИИ

THE MODERN AUTHENTICATION METHODS COMPARISON TECHNIQUE

O. Karelova
M. Lazareva

Summary. The research is aimed at developing a comparison technique that can be applied to the various groups of authentication methods. The result of the technique application is the most appropriate authentication method from the group in accordance with the selected criteria.

Keywords: authentication method, comparison technique, internet-users authentication, analytic hierarchy process, sessions, JSON Web Token.

Карелова Оксана Леонидовна
Доктор физико-математических наук, доцент
Московский Государственный Лингвистический Университет;
Российская академия народного хозяйства и государственной службы при Президенте РФ (Москва)
okarelova@yandex.ru
Лазарева Маргарита Владимировна
Бакалавр, Московский Государственный Лингвистический Университет (Москва)
shamelesss@list.ru

Аннотация. Исследование нацелено на разработку методики сравнения, которая может быть применима к различным группам методов аутентификации. Результатом применения методики является выбор наиболее подходящего метода аутентификации из группы в соответствии с выделенными критериями.

Ключевые слова: метод аутентификации, методика сравнения, аутентификация интернет-пользователей, метод анализа иерархий, сессии, JSON Web Token (JWT).

При анализе уже проведённых исследований по сравнению методов аутентификации и выбора наиболее эффективного и безопасного метода оказалось, что имеющиеся методы сосредоточены на сравнении факторов аутентификации и их комбинаций. Однако же фактор аутентификации и метод аутентификации понятия не идентичные, а работы, посвященных сравнению методов аутентификации, авторам найти не удалось. В настоящей статье предложена методика сравнения и выбора метода аутентификации, оптимального по многокритериальной оценке, на базе метода анализа иерархий. Этот инструмент широко используется, когда речь заходит о многокритериальном сравнении, именно поэтому он был выбран в качестве инструмента для исследования.

В первую очередь определимся с понятием двух терминов: фактор аутентификации и метод аутентификации. Эти термины часто ошибочно используются как синонимы. В данном исследовании используются определения, изложенные в ГОСТ Р 58833–2020 "Защита информации. Идентификация и аутентификация. Общие положения" [1]. Согласно этому документу, фактор аутентификации — это «вид (форма) существования информации, используемой при аутентификации» [1, п. 3.61]. Метод аутентификации, таким образом, следует понимать, как «реализуемое при аутентификации предопределенное сочетание факторов, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации» [1, п. 3.27]. Очевидно, что эти понятия существенно различаются и требуют различных подходов при их сравнении.

Для разработки методики сравнения методов аутентификации была проведена их классификация. Методы были классифицированы по области применения. Первая группа включает в себя методы, которые используются для аутентификации интернет-пользователей, эти методы представляют собой сессии и JSON Web Token (JWT). Ко второй группе отнесены методы аутентификации, которые основаны на алгоритмах электронной цифровой подписи. Вторая группа методов была использована для апробации построенной методики.

При рассмотрении методов аутентификации из первой группы были определены основные критерии, по которым производилась оценка этих методов. А именно — продолжительность времени действия ме-

Таблица 1. Сравнение методов аутентификации первой группы и их значения по критериям

		Сессии	JWT	JWT с сохранением состояния
	Генерируемый объём данных (сопровождает каждый запрос клиента), байт (К1)	40	320	364
	Необходимый объём хранилища для установленного количества пользователей, байт (К2)	32000	48	500
Безопасность	XSS (из 3-х факторов) (К3)	1	3	3
	CSRF (из 3-х факторов) (К4)	1	2	1
	Атака посредника (из 4-х факторов) (К5)	1	2	1

тода, объем сгенерированных данных и необходимость использования сторонних зависимостей [2]. Поскольку время истечения срока действия не может быть оценено как таковое, этот критерий не оценивается отдельно, а учитывается в блоке критериев безопасности, так как продолжительность срока действия влияет на степень подверженности рассматриваемым ниже атакам. Полный список условий, учитываемых при расчёте, включает в себя следующее:

- Опция JavaScript включена в браузере;
- Браузеру разрешено считывать и сохранять файлы cookie;
- JavaScript имеет доступ ко всем заголовкам запроса;
- Количество пользователей в системе — 100 пользователей;
- Количество полей токена для каждого пользователя — 5 (в скобках указаны поля в виде, в котором они записываются в токене): имя пользователя (username), реальное имя пользователя (name), права доступа (loginAs, например, администратор, пользователь, гость), адрес электронной почты (email), номер телефона (phone_number).

Результат сравнения (К3-К5) методов аутентификации первой группы и значения (К1-К2) по выделенным критериям представлены в таблице 1.

XSS (Cross-Site Scripting Attack) и CSRF (Cross-Site Request Forgery) обозначают атаку посредством межсайтового скриптинга и атаку межсайтовой подделки запроса, соответственно.

Критерий безопасности определяется степенью подверженности метода аутентификации выделенным атакам. Например, при рассмотрении атаки с использованием межсайтового скриптинга возможность установки флага HTTP-only для части запроса имеет решающее значение, поскольку этот флаг препятствует доступу JavaScipt к телу запроса. Полный список этих факторов описан ниже:

XSS:

1. Доступ JavaScript к телу данных аутентификации, определённый по умолчанию; 2. Возможность передачи данных в заголовке запроса; 3. Возможность установки флага HTTP-Only.

CRSF:

1. Размер объема данных, передаваемых в теле запроса (может ограничить возможность добавления заголовков для защиты от атаки); 2. Неограниченный срок действия; 3. Возможность мгновенного отзыва метода аутентификации.

Атака посредника:

1. Возможность нарушения целостности; 2. Утечка конфиденциальных данных (наличие конфиденциальной информации пользователя в теле метода); 3. Доступность для использования в течение длительного времени после перехвата (определяется временем истечения срока действия); 4. Возможность мгновенного отзыва метода аутентификации.

Все вышеперечисленные в таблице 1 критерии необходимо расположить в иерархическом порядке (от наиболее значимого к наименее значимому), что поможет в придании им весов при применении метода анализа иерархий.

XSS (К3) => CSRF (К4) => Атака посредника (К5) => Объем сгенерированных данных (К1) => Необходимый объем хранилища (К2)

В описанной последовательности критерии безопасности находятся выше в иерархической структуре, поскольку исследование в основном направлено на определение наиболее безопасного метода аутентификации.

Таблица 2. Матрица сравнений для критериев

	K1	K2	K3	K4	K5
K1	1	2	0,2	0,25	0,333333
K2	0,5	1	0,166667	0,2	0,25
K3	5	6	1	2	3
K4	4	5	0,5	1	2
K5	3	4	0,333333	0,5	1

Таблица 3. Матрица сравнений альтернатив по первому критерию

	A1	A2	A3	Сумма	a1
A1	1	2	3	6	0,529
A2	0,5	1	2	3,5	0,309
A3	0,333	0,5	1	1,833	0,162

Таблица 4. Итоговая таблица вычисления приоритетов

	a1	a2	a3	a4	a5	Приоритет
A1	0,529	0,162	0,5	0,4	0,4	0,438101
A2	0,309	0,529	0,25	0,2	0,2	0,244287
A3	0,162	0,309	0,25	0,4	0,4	0,317612

Среди критериев безопасности критерий, связанный с оценкой подверженности метода атаке типа "атака посредника", выбран как наименее значимый. Поскольку большинство соединений между клиентом и сервером защищены криптографическими методами (передаваемые данные зашифрованы), атака посредника становится трудной для реализации. Для проведения атаки CSRF необходимо, чтобы у пользователя была учетная запись на сервере, который будет скомпрометирован. Использование многофакторной аутентификации также снижает вероятность проникновения на сервер-жертву. Именно поэтому можно сказать, что перед реализацией атаки необходимо выполнить большое количество условий, что делает эту атаку менее эффективной, чем XSS.

На основании представленного порядка значимости критериев сформирована матрица сравнений для критериев, представленная в таблице 2. Веса присваиваются в соответствии со шкалой отношений метода анализа иерархий.

Kn (n=1,…,5) обозначает номер критерия в списке, представленном в таблице 1.

Матрица является согласованной, так как при расчёте отношение согласованности (ОС) получилось меньше 0,10. Каждому критерию был присвоен вес, который отражает уровень значимости критерия по отношению к другим критериям [3]. На основании проставленных весов определяется вектор приоритетов — b^{T} (0,086 0,048 0,384 0,283 0,199).

Далее проводится оценка методов аутентификации по каждому из критериев. Пример оценки по первому критерию приведен в таблице 3. Вектор a1 — вектор приоритетов альтернатив по первому критерию.

Оптимальный по совокупности критериев метод аутентификации выбирается в соответствии с результатами, представленными в сводной таблице (табл. 4) метода анализа иерархий, которая отражает расчеты, проведенные по каждому критерию.

Сессии выбираются как наиболее предпочтительный метод аутентификации в рамках первой группы рассматриваемых методов, то есть группы методов, направленных на аутентификацию интернет-пользователей.

Таким образом, разработанная методика включает в себя следующие этапы:

1. Сравнение алгоритмов работы каждого метода внутри выделенной группы методов аутентификации. Различия, определенные в ходе сравнения, используются для выработки критериев, оценивающих функциональность метода.
2. Поскольку исследование нацелено на создание методики, которая сравнивает методы на основе

аспекта безопасности, следует определить соответствующие критерии безопасности для рассматриваемых методов аутентификации.

3. Чтобы провести различие между более значимыми критериями и менее значимыми, необходимо расположить их в иерархическом порядке. Таким образом, отношения между критериями становятся более прозрачными в процессе взвешивания.
4. Выбранным критериям, в соответствии со шкалой отношений метода анализа иерархий, выставляются веса.
5. По методу анализа иерархий проводится сравнение методов аутентификации по каждому критерию.
6. Решение по выбору наиболее подходящего метода аутентификации принимается на основе результатов вычисления приоритета.

Результаты, полученные в исследовании, могут быть применены для определения наиболее подходящего метода аутентификации в рамках групп методов, отличных от тех, что рассмотрены в статье. Группы уже проанализированных методов могут помочь в выборе метода аутентификации при разработке системы информационной безопасности. Более того, методика в дальнейшем может быть усовершенствована посредством учета числовых значений методов по критериям, а не только их рангов.

ЛИТЕРАТУРА

1. ГОСТ Р 58833–2020. Защита информации. Идентификация и аутентификация. Общие положения.
2. Madden, Neil. API Security in Action / Manning Publications Co, 2020–553 p.
3. Саати Т. Принятие решений, метод анализа иерархий / Москва «Радио и связь», 1993–278 с.

Журнал «Современная наука: актуальные проблемы теории и практики»

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации