3 Экстремальное программирование — реальность и мифы [Электронный ресурс]: элек- трон. текстовые дан – Режим доступа: http://skipy.ru/philosophy/xp.html

4 Поппендик М. Бережливое производство программного обеспечения: от идеи до прибыли [Текст] / М. Поппендик. — М. : «Вильямс», 2009. – 256 с.

5 Кон М. Scrum: гибкая разработка ПО [Текст] / М. Кон — М. : «Вильямс», 2007. – 576 с.

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ СЕРВИСОВ АУТЕНТИФИКАЦИИ ПУТЕМ ПРОВЕДЕНИЯ ДОПОЛНИТЕЛЬНОЙ ИДЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ОПТИМАЛЬНОГО ПРИЗНАКОВОГО ПРОСТРАНСТВА

А.Ю. Исхаков, С.Ю. Исхаков, Р.В. Мещеряков
Томск (Томский государственный университет систем управления и радиоэлектроники)
iskhakovandrey@gmail.com

INCREASE IN SECURITY OF AUTHENTICATION SERVICES THROUGH ADDITIONAL IDENTIFICATION USING OPTIMAL FEATURE SPACE

A.Y. Iskhakov, S.Y. Iskhakov, R.V. Meshcheryakov
Tomsk (Tomsk State University of Control Systems and Radioelectronics)

Abstract. The research focuses on topical issue of the Internet security. In particular, the issue of level increase in security of authentication services through additional identification using optimal feature space is being considered. This article is devoted to the practical application of additional identification technologies in authentication services. The paper presents sets of informative features characterizing the access subject. A classification of methods for identifying the user's work environment is proposed. The article presents the experimental results of intercomparison between scientifically-grounded methods and technologies for identifying the user's work environment.

Keywords: authentication; identification; information security; IoT; identification methods; attribute; user; browser fingerprint; cookies.

Введение. Сегодня глобальная сеть Интернет день является одним из основных инструментов массовых коммуникаций. Ее стремительное развитие неразрывно связано с новыми научными открытиями и технологическими инновациями в различных сферах it-индустрии. Данные обстоятельства способствуют развитию информационных систем самого разного профиля, обеспечивающих возможность удаленного взаимодействия с пользователями. С увеличением объема пользовательских данных в сети неразрывно растет и количество различных киберугроз [1].

Эта проблема в частности характерна для инфраструктуры Интернета вещей (IoT) [2, 3]. Одной из важных задач в обеспечении защиты элементов сетевых систем, в том числе таких как IoT, является реализация эффективного функционала по контролю и управлению доступом для пользователей, осуществляющих удаленные подключения к элементам сети, а также smart-устройствам [4]. В частности, в рамках данного исследования будут рассмотрены вопросы повышения защищенности сервисов аутентификации путем проведения дополнительной идентификации субъектов доступа.

Необходимость проведения дополнительной идентификации. Рассмотрим перспективную инфраструктуру облачного видеонаблюдения в концепции IoT. Подобные комплексы давно перестали быть просто системами, транслирующими видео с камеры на устройство для просмотра. Сегодня настала эпоха облачного видеонаблюдения: удаленного smart-мониторинга, не нуждающегося в постоянном контроле оператора. Активное видеонаблюдение способно анализировать видеопоток в режиме реального времени и уведомлять пользователя о возможных инцидентах.

Зачастую ограничение доступа к панели управления подобной информационной системой посредством стандартных способов аутентификации недостаточно. Это может быть связано с бизнес-процессами функционирования объекта применения. В таких случаях администраторы информационной безопасности вынуждены интегрировать дополнительные механизмы идентификации посетителей. В то же время существуют способы получения данных, характеризующих рабочую среду пользователя, то есть данные об операционной системе, шрифтах, параметрах экрана, плагинах, посещенных ссылках и т.п. Известны попытки использования перечисленных данных в качестве признаков идентификации [5–7]. Однако использование такой технологии влечет за собой увеличение объема трафика, что не приемлемо для типичных представителей IoT-инфраструктуры.

Таким образом, целями данной работы является определение оптимального признакового пространства и способа дополнительной идентификации, позволяющего повысить достоверность отождествления пользователей с имеющимися записями в базе данных информационной системы, применяемого в сервисе аутентификации.

Классическим и наиболее популярным вариантом создания удобного и кроссплатформенного интерфейса для взаимодействия с пользователям IoT-инфраструктуры является использование веб-ориентированных технологий с применением таких языков как HTML, CSS, JavaScript и др. Методы аутентификации к подобным приложениям разделяются в зависимости от типа ресурса, структуры организации сети, а также технологии, которая используется в процессе распознавания. В таблице 1 приведены наиболее популярные методы аутентификации.

Таблица 1 – Методы аутентификации в веб-приложениях

Метод	**Способ реализации / протоколы**	**Назначение**
По паролю	HTTP authentication (Basic, Digest, NTLM, Forms)	Аутентификация пользователей
По одноразовым паролям (OTP)	Forms	Усиленная аутентификация пользователей
По сертификатам	SSL/TLS	Строгая аутентификация пользователей в безопасных приложениях; аутентификация сервисов
По ключам доступа	–	Аутентификация сервисов и приложений
По «токенам»	SAML, WS-Federation, OAuth, OpenID Connect	Делегированная аутентификация пользователей; делегированная авторизация приложений

Многообразие вышеперечисленных методов позволяет применять дифференцированный подход к построению сервисов аутентификации в зависимости от поставленных задач и выделяемых ресурсов. Принимая во внимание особенности функционирования некоторых комплексов, следует отметить необходимость разработки способа дополнительной идентификации субъекта доступа, позволяющего выявлять подозрительные сеансы пользователей с других систем. Одним из примеров таких случаев является рассматриваемая авторами локальная IoT-инфраструктура облачного видеонаблюдения, ограниченная вычислительными ресурсами. В такой системе отсутствует возможность установки полноценной системы обнаружения вторжений (IDS) [8], способной выявлять факты аномальной деятельности пользователей.

Пространство идентификационных признаков. В рамках проведенного исследования авторским коллективом была сформирована следующая классификация методов идентификации рабочей среды пользователя [9]:

1. Установка уникального идентификатора пользователя

Методы основаны на применении следующих признаков (характеристик):

– Cookies – небольшой фрагмент данных, хранимый на компьютере пользователя;

– Local Shared Objects (LSO) – тип метаданных, которые хранятся в виде файлов на компьютере каждого пользователя. Сегодня все версии Flash Player используют LSO;

– Isolated Storage – изолированное хранилище Silverlight. Как и в LSO, с технической точки зрения здесь нет каких-либо препятствий для хранения идентификаторов сессии;

– HTML5-хранилища (localStorage, File API и IndexedDB), предназначеные для обеспечения хранения произвольных порций данных, привязанных к конкретному ресурсу;

– Объекты кеша браузера;

– Абстрактный идентификатор ETag (Тэг версии закешированного документа);

– Заголовок Last-Modified (Дата версии закешированного документа);

– Application cache (HTML5) – набор функций для продвинутого кэширования ресурсов web-приложения;

– SDHC-словари;

– Использование внутреннего DNS-кеша браузера;

– Прочие механизмы хранения (window.name или session.storage);

– Использование особенностей протоколов – например, Origin Bound Certificate, TLS;

2. Использование вычисленных характеристик автоматизированной системы пользователя.

– «отпечатки» браузера – объединение набора параметров, доступных в среде браузера. Каждый из идентификаторов по отдельности не представляет никакого интереса, но их совокупность образует уникальное для каждой автоматизированной системы значение;

– «сетевые отпечатки» – значения внешнего и локального ip-адреса, номера портов для исходящих TCP/IP-соединений, сведения об используемом Proxy-сервере и т.д.

3. Анализ динамических идентификационных признаков (поведенческий анализ).

Такой метод позволяет идентифицировать клиентов между различными сессиями браузера, профилями и в случае приватного просмотра. Используются, например:

– характеристики жестов мыши;

– частота и продолжительность нажатия клавиш;

– данные с акселерометра;

– уровень zoom, использование специальных возможностей.

Проведение эксперимента. Для исследования были взяты следующие научно-обоснованные методы и технологии идентификации рабочей среды пользователя:

1. Метод идентификации с использованием компонентного профиля, представляющего собой кортеж наиболее информативных данных о рабочей среде пользователя [11].

2. Метод Cross-Browser Fingerprinting (CBS), основанный на профилировании компьютера по времени выполнения различных графических операций в минуту [11]

3. Технология Panopticlick Fingerprints.

4. Технология Evercookie [12], объединяющая в себе HTTP cookie, Flash cookie, Silverlight Isolated Storage, PNG + canvas cookie, session storage, local storage, Indexed DB, ETag, Java Persistence.

5. Технология FingerprintJS.

Согласно [13] данные методы находят широкое практическое применение в задачах идентификации пользователей в сети Интернет. С целью получения значений статистических характеристик был осуществлен сбор экспериментальных данных на базе 3 информационных систем облачного видеонаблюдения за открытыми объектами массового пребывания людей в течение 3 месяцев. В выбранных системах применяется базовая аутентификация по паролю. На рис. 1 представлен результат выполнения эксперимента по оценке времени быстродействия.

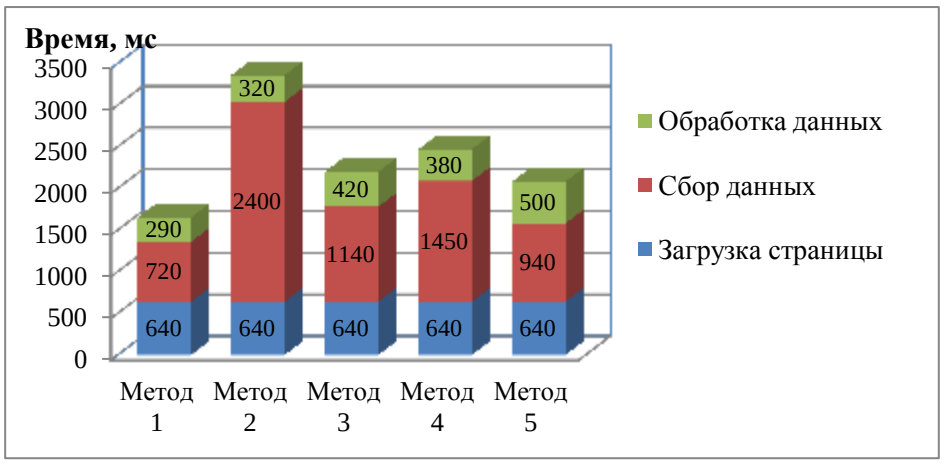

Рис. 1. Результаты тестирования быстродействия методов

Данные получены при анализе 15 000 запросов. Среднее значение первого запроса к основному содержимому страницы занимает одинаковое время. Процесс сбора данных у метода №2 значительно превышает остальных в связи с необходимостью проведения множества графических операций (например, нанесение растрового изображения на грань куба средствами WebGL с аппаратным видеоускорением).

Далее была проведена оценка зависимости количества идентифицированных пользователей от уровня внесенного шума. Под шумом в данной работе понимаются намеренно или случайно искаженные данные, которые не могут служить основной для идентификации.

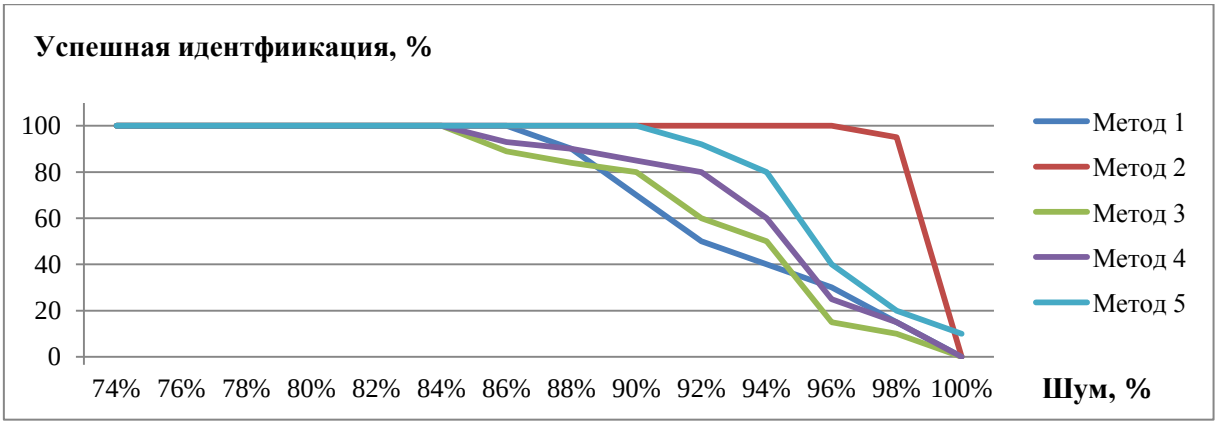

Рис. 2. Зависимость эффективности работы методов от степени зашумленности выборки

Эксперимент показал, что все методы показывают максимальную степень эффективности при условии зашумленности выборки до 84% включительно. При внесенном шуме более 90% все методы кроме 2 и 5 резко ухудшают свои результаты. При 95% искаженных данных к числу робастных можно отнести лишь Cross-Browser Fingerprinting. Например, при 96% показателя зашумленности процент корректной идентификации у методов 1,3-5 не достигает и 40%. Метод №2 является наилучшим с точки зрения достоверности идентификации пользователей, а метод №1 – с точки зрения быстродействия. Однако, необходимо учитывать, что в вышеприведенном случае точность идентификации влияет на скорость передачи контента. Поэтому практическое применение метода №2 в таких сервисах как облачное видеонаблюдение приведет к значительным задержкам в работе пользователей. Таким образом, авторам представляется целесообразным комбинирование методов 1 и 2 с учетом особенностей бизнес-процессов применения информационной системы. В процессе исследования вышеперечисленных технологий были выявлены следующие недостатки массового характера:

1. Смена политики выпуска новых версий браузеров в последнее время снизила эффективность использования атрибута UserAgent.

2. Продукция фирмы Apple (Iphone, Ipad и др) характеризуются высокой степенью аппаратной унификации. Это означает, что тот байтовый массив, полученный с Canvas Fingerprint, будет одинаков для IPhone (с установленной операционной системой IOS до версии 8.1). Следствием этого является снижение точности идентификации.

3. Большое количество компьютеров, использующих старые версии браузера Internet Explorer, не позволяют получить список установленных плагинов.

Заключение. Если ранее применяемые технологии позволяли с приемлемой вероятностью определять пользователя одного браузера, то современные методы позволяют осуществлять достоверную идентификацию пользователей, намеренно применяющих несколько разных браузеров. Безусловно, такие способы анонимизации как использование сетей Tor, позволят обойти подобные проверки дополнительной идентификации. Однако, список выходных узлов данной технологии опубликован и постоянно обновляется. Разработчику сервисов аутентификации необходимо автоматизировать обновление данного реестра и настроить соответствующую блокировку.

Результаты проведенных экспериментов показали, что на сегодняшний день не существует универсального инструмента, позволяющего проводить достоверную дополнительную идентификацию пользователей при минимальной трудоемкости. Как и в случае с самой технологией аутентификации необходимо применять дифференцированный подход к выбору оптимального признакового пространства, позволяющего повысить достоверность отождествления пользователей с имеющимися записями в базе данных информационной системы, применяемого в сервисе аутентификации.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в рамках мероприятия 1.3 ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение о предоставлении субсидии № 14.577.21.0172 от 27 октября 2015 г.; уникальный идентификатор RFMEFI57715X0172).

ЛИТЕРАТУРА

1. Hsu S.H.Y., Dick S.J. Information sharing & cyber threats // 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). – 2017. – Pp. 89 - 94.

2. Gupta K., Shukla S. Internet of Things: Security challenges for next generation networks // 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). – 2016. – Pp. 315 - 318.

3. Zhao K., Ge L. A Survey on the Internet of Things Security // 2013 Ninth International Conference on Computational Intelligence and Security. – 2013. – Pp. 663 – 667.

4. Iskhakov A., Meshcheryakov R., Ekhlakov Yu. The Internet of Things in the security industry // INTERACTIVE SYSTEMS: Problems of Human - Computer Interaction. - Collection of scientific papers. – 2017. – Pp. .161 - 168.

5. Бессонова Е. Е., Зикратов И. А., Колесников Ю. Л., Росков В. Ю. Способ идентификации пользователя в сети Интернет // Научно-технический вестник информационных технологий, механики и оптики. − 2012. − Вып.3. − С. 133-137.

6. Кантор И. Способы идентификации в интернете [Электронный ресурс]. URL: http://javascript.ru/unsorted/id (дата обращения: 12.10.2017).

7. Eckersley P. How Unique Is Your Web Browser? [Electronic resource] URL: https://panopticlick.eff.org/browser-uniqueness.pdf (access date: 03.10.2017).

8. Iskhakov S., Shelupanov A., Meshcheryakov R. Simulation modelling as a tool to diagnose the complex networks of security systems // Journal of Physics: Conference Series. – 2017.

9. Жуков А. Фингерпринтинг браузера. Как отслеживают пользователей в Сети [Электронный ресурс]. URL: https://xakep.ru/2015/01/30/user-web-tracking-howto/ (дата обращения: 10.10.2017).

10. Бессонова Е.Е. Метод идентификации пользователей в сети Интернет с использованием компонентного профиля, дисс. на соиск. степ. к-та. техн. наук [Электронный ресурс]. URL: https://isu.ifmo.ru/index/B996F9609F0750E3BBDF52445A22C FC1 (дата обращения: 14.10.2017).

11. Cao Y., Li S., Wijmans E. (Cross-)Browser Fingerprinting via OS and Hardware Level Features Conference: Network and Distributed System Security Symposium, 2017 [Electronic resource]. URL: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf (access date: 14.10.2017).

12. Fleishman G. How to kill the evercookie and supercookie, the cockroaches of tracking, 2017 [Electronic resource] URL: https://www.macworld.com/article/3152056/privacy/ how-to-kill-the-evercookie-and-supercookie-the-cockroaches-of-tracking.html (access date: 14.10.2017).

13. Методы идентификации пользователя в Интернете, 2017 [Электронный ресурс]. URL: https://serfmoney.ru/cpa/metody-identifikatsii-polzovatelya-v-internete/ (дата обращения: 15.10.2017).

АНАЛИЗ УЯЗВИМОСТЕЙ В ЭНЕРГОЭФФЕКТИВНЫХ СЕТЯХ ДАЛЬНЕГО РАДИУСА ДЕЙСТВИЯ НА ПРИМЕРЕ LORAWAN

С.Ю. Исхаков, А.А. Исхакова, Р.В. Мещеряков
(г. Томск, Томский государственный университет систем управления и радиоэлектроники)
e-mail: iskhakov.sy@gmail.com

ANALYSIS OF VULNERABILITIES IN LOW-POWER WIDE-AREA NETWORKS BY EXAMPLE OF THE LORAWAN

Sergey Iskhakov, Anastasia Iskhakova, Roman Meshcheryakov
(Tomsk, Tomsk State University of Control Systems and Radioelectronics)

Abstract. The increasing number of automated systems using the global network for management has led to the need to search for new technologies for transmitting data from various sensors over long distances with minimal energy consumption. Today, there are several similar technologies on the market that claim to be the world standard in the concept of the Internet of things, but none of them has yet been studied in detail from the point of view of security. This article is devoted to the analysis of one of the most common protocols in order to identify potential vulnerabilities.

Keywords: Internet of Things; modulation; network; vulnerability; replay attack; spoofing.

Введение. В последнее время наблюдается интенсивное распространение концепции Интернета вещей (IoT) [1,2], которую можно определить как глобальную динамическую сетевую инфраструктуру, где физические и виртуальные «вещи» имеют идентификаторы и физические атрибуты, и интегрируются в информационную сеть, используя различные интерфейсы. Все большее внимание привлекают технологии, позволяющие создавать энергоэффективные сети дальнего радиуса действия (Low-Power Wide-area Network, LPWAN) [4]. Представим жилой многоквартирный дом, где системы водоснабжения и электрификации подключены к IoT и передают показания в автоматическом режиме на станцию мониторинга. Во-первых, если для электросчетчика легко обеспечить постоянное питание, то прокладка кабелей к счетчикам воды сводит на нет всю концепцию использования беспроводных технологий. Поэтому радиомодуль счетчика должен работать от локального источника энергии (батарейки). Энергопотребление современных модулей Wi-Fi [1] и LTE [4] обуславливает