РАЗРАБОТКА СИСТЕМЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ ПРИ СОЗДАНИИ ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ

Таджибаев Жавохир Шухрат угли

[*] *Магистр, факультет кибербезопасности, Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, Узбекистан*

Аннотация: *Аутентификация получает огромное внимание со стороны исследовательского сообщества и доказывает, что является интересной областью в сегодняшнюю эпоху. Аутентификация пользователей является серьезной проблемой, поскольку люди хранят свои личные данные на устройствах. Для усиления аутентификации пользователей введены пароли. В прошлом текстовый пароль был традиционным способом аутентификации, но у этого метода есть определенные недостатки. В качестве альтернативы был введен графический пароль, который использует изображение или набор изображений для создания пароля. В будущем такие подходы должны поддерживать надежность и потреблять меньше энергетических ресурсов, чтобы стать пригодными для зеленого Интернета вещей (IoT). Точно так же различные графические механизмы аутентификации по паролю использовались для повышения безопасности и удобства использования пользователями. В этой статье мы проводим обширный обзор существующих подходов к аутентификации с помощью графического пароля, чтобы выделить проблемы, которые необходимо решить для «зеленого» Интернета вещей. По сравнению с другими существующими опросами, цель состоит в том, чтобы закрепить метод графического пароля и выявить проблему, связанную с ним. Кроме того, это исследование также выявит уязвимости графического пароля против нескольких потенциальных атак. Мы также рассмотрели сильные и слабые стороны каждого метода, а также направления будущих исследований. В этом исследовании также оценивается удобство использования каждого подхода с учетом обучаемости, запоминаемости и т. д., а также представлен сравнительный анализ с безопасностью.*

Ключевые слова: *компьютерная аутентификация, графический пароль, компьютерная безопасность.*

Введение. Безопасная связь и аутентификация продуктов создают серьезные социальные проблемы. Решением может стать система оптической аутентификации, основанная на физических неклонируемых функциях (PUF). Использование PUFs в системе защиты от подделок позволит решить проблему экономических потерь в миллиарды долларов, вызванных подделкой, и потенциально может спасти жизни, если они будут использоваться для гарантии подлинности лекарств. Случайность, присущая PUF, может быть использована для невзламываемого шифрования с

открытым ключом. Ключ дешифрования невозможно угадать, а поскольку PUF по определению не может быть скопирован, только владелец ключа может расшифровать зашифрованное сообщение. Здесь мы представляем новую оптическую систему аутентификации, основанную на PUF-структурах цеолитовых меток, легированных лантанидами, в полимерных пленках, которые считываются с использованием изображений легирующих добавок лантанидов, выбранных при возбуждении. Система демонстрируется в контексте системы защиты от подделок.

В борьбе с контрафактной продукцией все установленные технологии используют метки, которые являются результатом детерминированного процесса. Как следствие, все они полагаются на ограниченный доступ к чернилам или технологии печати, что делает их уязвимыми для подделок — даже метки ДНК легко считываются и копируются, если имеется подходящий стимул. Представленный здесь высокозащищенный метод кодирования отличается по своей природе, поскольку он использует статистически уникальные физические ключи, основанные на PUF, которые основаны на недетерминированных, случайных характеристиках метки защиты от подделки, что делает невозможным дублирование даже производителем, не говоря уже о фальшивомонетчиках.

Представленная система аутентификации основана на физических ключах, созданных из физических односторонних функций, более известных как PUF. Мы создаем эти уникальные случайные узоры в стохастическом процессе, когда метки, нанесенные на тонкую полимерную пленку, создают случайный узор на выбранной подложке. Путем визуализации выбранной области тонкой пленки создается уникальный физический ключ. Такой ключ PUF можно прикрепить к каждой блистерной упаковке таблеток или дизайнерской ручной сумке, и каждый продукт будет иметь уникальный ключ. Все физические ключи считываются, а их цифровые ключи хранятся в базе данных, что позволяет однозначно идентифицировать каждый продукт по всей цепочке поставок.

Физический ключ считывается с помощью трех энергетически близко расположенных синих лазерных линий, каждая из которых избирательно возбуждает разные ионы лантанидов. Излучение, следующее за избирательным возбуждением, используется для изображения ключа. Управление возбуждающим светом, а не испускаемым светом, разрешает различные теги, используемые для формирования уникального шаблона, который является ключом PUF. На каждой длине волны возбуждения возникает уникальный уникальный случайный шаблон, а оцифрованный и объединенный шаблон образует уникальный цифровой ключ. Этот новый метод считывания случайного шаблона отличается от известных методов оптического мультиплексирования, которые считываются путем анализа цветового состава излучаемого света. Когда этот новый режим считывания сочетается с уникальными параметрами для оцифровки и сравнения показаний, мы создали защищенную от несанкционированного доступа систему оптической аутентификации.

Здесь мы демонстрируем концепцию оптической аутентификации с разрешением возбуждения для защиты от подделок с использованием физических ключей, изготовленных из цеолитов, легированных ионами европия (III), тербия (III) или диспрозия (III), иммобилизованных в тонкой пленке поливинилового спирта (ПВС). Мы используем узкое поглощение линии лантаноидов и эмиссия, ориентированная на лантаниды, для разрешения до трех бинарных откликов, в зависимости от наличия или отсутствия данного лантаноида в данном пикселе. Используя три иона лантанида (III), мы достигаем очень высокой кодирующей способности. Кодирующая способность нашей системы (ср) определяется количеством возможных ответов, демонстрируемых случайным образцом. С тремя ионами лантанида (III) мы можем получить семь различных откликов, которые мы визуализируем, используя стандартную цветовую схему (с = 7; RGB-CMYK). В представленных здесь примерах мы отображаем область размером 60 пикселей × 60 пикселей (р = 3600), что дает максимальную кодирующую способность предлагаемой системы аутентификации, равную 73600. Поскольку кодирующая способность случайного шаблона бесконечна для всех практических целей. , никогда не будет двух одинаковых ключей, что гарантирует невозможность копирования физических ключей.

Материалы: все данные, необходимые для оценки выводов статьи, представлены в статье и/или дополнительных материалах. Дополнительные данные, относящиеся к данной статье, могут быть запрошены у авторов.

Методы: Буквенно-цифровой пароль — это старый традиционный распространенный метод аутентификации. Практически этот традиционный метод является слишком небезопасной системой. Например, злоумышленник может выбрать легко угадываемый пароль пользователя, если пользователь не использует надежный пароль. Пользователь может использовать один и тот же пароль для нескольких устройств или сайтов. Это все небезопасная характеристика для обычных пользователей. И аутентификация является одним из важных моментов безопасности, где пользователь несет активную ответственность за безопасность своей личной информации. Если мы используем старую традиционную систему паролей, тогда может возникнуть возможность атаки по словарю, атаки грубой силы.

Результаты: Очерчена полная система аутентификации. Для реализации примера мы предлагаем включить метки в полимер, используемый для блистерной упаковки; таким образом, физический ключ — это просто выбранная область пакета. Полная система аутентификации содержит три уровня безопасности: физический ключ, программное обеспечение для оцифровки, включая определение шумоподавления и перекрестных помех, а также критерии приемлемости для сравнения двух цифровых ключей с одним и тем же физическим ключом. Критерии приемлемости будут сильно зависеть от аппаратного обеспечения считывателя. При использовании нашей установки и схемы RGB+K мы предлагаем критерий приемки,

при котором допустимая погрешность составляет 40 % в каждом канале. Это приводит к ложноположительной вероятности 3,6 × 10–96, что приемлемо для всех практических целей (см. Дополнительные материалы). Допустимая погрешность допускает небольшие различия между отдельными считывателями, используемыми в разных точках цепочки поставок. Поскольку время считывания невелико, а цифровая обработка выполняется быстро, ложные срабатывания можно полностью исключить, выполнив операцию аутентификации в трех экземплярах. Обратите внимание, что критерии приемлемости должны быть адаптированы к фактически используемым меткам защиты от подделки и оборудованию. Чтобы продемонстрировать систему аутентификации как средство защиты от подделок, мы внедрили и протестировали один набор из двух критериев приемки. обобщает требования системы защиты от подделок, где продукты должны быть аутентифицированы на всех этапах цепочки поставок, и включает пример, когда мы бросили вызов нашей системе с двумя продуктами с подлинным и поддельным ярлыком защиты от подделки. Тег PUF был зарегистрирован в точке происхождения путем считывания физического ключа и сохранения копии цифрового ключа. Затем цифровой ключ использовался для аутентификации физического ключа, который был пересчитан четыре раза, чтобы проиллюстрировать различные точки в цепочке поставок. Физические ключи, которые не совпадали с цифровым ключом, не были аутентифицированы (см. Дополнительные материалы).

Заключение. Таким образом, мы продемонстрировали оптическую систему аутентификации, использующую уникальные оптические свойства трехвалентных ионов лантанидов, PUF, современные оптические технологии и криптографические подходы. Система оптической аутентификации может использоваться для невзламываемого шифрования, но была продемонстрирована в целях защиты от подделок. При использовании в качестве системы защиты от подделок производитель маркирует продукт уникальным физическим ключом и записывает цифровой ключ, соответствующий ключу PUF, в общедоступную базу данных, доступную только для чтения. Количество уникальных физических ключей почти бесконечно, и случайно идентичные теги защиты от подделок не встречаются. Кроме того, поскольку ключ PUF уникален и не может быть скопирован, нет необходимости в секретности. Затем продавцы и конечные пользователи могут проверить подлинность продукта с помощью магазинных или персональных считывателей, которые, зная тип продукта, ищут цифровой ключ в разделе базы данных соответствующего производителя. Большое пространство параметров случайно сгенерированных PUF-ключей, изготовленных из доступных материалов, обеспечивает простой подход к аутентификации товаров народного потребления, лекарств, паспортов или электронных компонентов, подвергшихся подделке. Надежные физические клавиши могут быть либо привиты к изделию, либо поставляться в виде тонких фильмы. Фундаментальные свойства ионов лантанидов,

используемых в визуализации с выбранным возбуждением, не могут быть сымитированы, структуры не могут быть напечатаны, а ключи продуктов зарегистрированы надежными производителями. Все три факта по отдельности сделают метод защищенным от несанкционированного доступа. Экономическая выгода от защиты прав на товарный знак и интеллектуальную собственность значительна, а использование изображений цеолитов, легированных лантанидами, с выбранным возбуждением для обеспечения подлинности лекарств спасет жизни.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

[1] Графическая аутентификация по паролю. Шраддха М. Компьютерный факультет Гурав Мумбайского университета RMCET Ратнагири, Индия. Лина С. Гаваде Компьютерный факультет Университета Мумбаи RMCET Ratnagiri, Индия, IEEE, 2014 г.

[2] Усовершенствование системы аутентификации пароля с использованием графических изображений. Амол Бханд, Вайбхав десале Савитрибай Пхуле Университет Пуны, факультет вычислительной техники Свати Ширке Инженерная школа NBN Sinhgad, Пуна, 16-19 декабря 2015 г.

[3] Метод графической аутентификации пароля, устойчивый к серфингу через плечо. Г-жа Ааканша С. Гокхалеа, профессор Виджая С. Вагмареб.

[4] Новая графическая схема пароля, устойчивая к серфингу через плечо. Школа компьютерных наук Уве Айкелина Ноттингемского университета Ноттингем, NG8 1BB, Великобритания

[5] Сведение к минимуму атак с использованием плечевого серфинга с использованием схемы графического пароля на основе текста и цвета. Проф. С.К. Сонкар, проф. Р.Л. Пайкрао, проф. Авадеш Кумар, г-н С.Б. Дешмукх, кафедра вычислительной техники, кафедра компьютерной инженерии, инженерный колледж Амрутвахини, февраль – 2014 г.

[6] Графический пароль против программ-шпионов и атак через плечо. Эльхам Дарбанян Магистр технических наук, Колледж электронного обучения Ширазского университета, Гх. Дастгайби Фард Факультет компьютерных наук и инженерии, Колледж электротехники, вычислительной техники и инженерии Ширазского университета, июнь 2015 г.

[7] Текстовая графическая система паролей для скрытия серфинга через плечо. Хазима Ирфан, Ага Анас, Сидра Малик, Саниха Амир Департамент компьютерных наук Институт информационных технологий COMSATS, Исламабад, Пакистан, 13 января 2018 г.

[8] Графическая модель проверки подлинности пароля для мобильных устройств. Тео Джу Фонг, Азвин Абдулла, Школа вычислительной техники и информационных технологий Джанджи Новой Зеландии, Университет Тейлора, Субанг Джая, Селангор, Малайзия, 2019 г.

[9] Безопасность при графической аутентификации. Роберт Г. Риттенхаус, Джунаид Ахсенали Чодри и Малри Ли Департамент компьютерных наук и инженерии, Катарский университет, Доха, Катар, май 2013 г.