Имитационное моделирование постбиометрического метода аутентификации на основе данных о пользователе

А. А. Грушо, М. И. Забежайло, Д. В. Смирнов, Е. Е. Тимонина

***Аннотация* — Аутентификационные данные, такие как пароль, ключевое слово, номер паспорта и т.д., аутентификационный материал, такой как биометрический отпечаток пальца, лица и т.д., аутентификационные предметы, такие как телефон, паспорт, токен и т.д., могут быть подсмотрены, подделаны и переданы злоумышленнику. Существующие системы многофакторной аутентификация являются «конечно-факторными» т.е. количество факторов, используемых в системе аутентификации и перечисленных выше, конечно и заранее известно. Данными уязвимостями пользуются хакеры, разрабатывающие многоканальные вирусы, с помощью которых скрытно и удаленно контролируется одновременно компьютер и смартфон жертвы. Контролируя смартфон жертвы, хакер может скрытно читать СМС пароли или иногда push уведомления. Таким образом, существующие четыре группы факторов аутентификации, такие как когнитивные, основанные на знании субъекта, биометрические, основанные на физиологии и поведении субъекта, факторы, основанные на местоположении субъекта, и факторы владения информацией или токеном имеют следующие недостатки:**

(1) секрет отделим от пользователя, и находится на клиенте,

(2) пароль возможно повторить,

(3) биометрию возможно подделать,

(4) местоположение возможно подстроить по сговору.

В работе предлагается новый метод проведения аутентификации пользователя, лишенный данных недостатков, с помощью случайных вопросов, созданных на основе имеющихся о пользователе данных. Решение об успешности процедуры аутентификации пользователя (полифакторная аутентификация) принимается по результатам его ответов. Основная проблема предложенного метода аутентификации заключатся в том, чтобы найти оптимальные параметры системы аутентификации, реализующей предложенный алгоритм и самого алгоритма, реализующего создание вопросов. Цель работы – найти такие параметры.

Статья получена 03 апреля 2019.
Работа поддержана РФФИ (проект № 18-29-03081-мк).
А. А. Грушо, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: grusho@yandex.ru).
М. И. Забежайло, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: m.zabezhailo@yandex.ru).
Д. В. Смирнов, ПАО Сбербанк России, dvlsmirnov@sberbank.ru.
Е. Е. Тимонина, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: eltimon@yandex.ru).

***Ключевые слова* — Информационная безопасность, информационные пространства, имитационное моделирование, полифакторная аутентификация, параметры работоспособности алгоритма.**

Введение

В наше время набирают популярность методы идентификации/аутентификации (И/А), основанные на биометрических технологиях (биометрия). Биометрию встраивают в различные персональные устройства, т.е. смартфоны, персональные компьютеры и в информационные системы, т.е. системы контроля доступа, аутентификации и т.д. Ряд государств осуществляет внедрение биометрических систем И/А на государственном уровне [1]. Биометрия становится популярной, потому что она в настоящее время имеет несколько основных преимуществ над другими методами И/А: простота использования и низкий риск потери, трудоемкость подделки биометрического идентификатора клиента. Тем не менее, при своих явных преимуществах биометрия имеет и серьезные недостатки, один из которых – это невозможность обновить украденные биометрические идентификаторы. Злоумышленник сможет предъявлять украденные биометрические идентификаторы на протяжении всей жизни жертвы, при этом биометрические идентификаторы жертвы не могут быть обновлены или переизданы, как, например, пароль.

В связи с вышеизложенным, существует потребность в альтернативных способах И/А для случаев компрометации самой технологии биометрической И/А или компрометации биометрических идентификаторов клиентов. В качестве альтернативы биометрии возможно рассмотреть два направления И/А:

- существующие методы И/А, такие как пароль, СМС, токен и т.д. или их комбинации;
- принципиально новые или постбиометрические методы.

Разработкой таких принципиально новых методов аутентификации в отношении биометрии занимались авторы работ [2-10], в которых предлагалось:

- производить И/А на основе сравнения схожести эталонной фотографии и фотографии, предоставленной пользователем в систему И/А [3];
- применять методы геймификации, чтобы помочь пользователю запомнить ответы на сложные вопросы, в результате которых принимается решение о прохождении процедуры И/А [4];
- использовать координаты геолокации с привязкой ко времени пользователя мобильного устройства [5] как фактор для проведения И/А;
- проводить И/А пользователя на основании данных взаимодействия пользователя с его мобильным устройством [6];
- использовать персональную камеру для сбора изображений, которые запомнились пользователю в течение дня, и впоследствии использовать собранные изображения для проведения И/А [7];
- использовать мобильные устройства с установленным ПО как второго фактора И/А [8];
- использовать данные мобильного устройства как фактор И/А [9];
- использовать данные местоположения пользователя и сервиса, на которые пользователь подписан как фактор И/А [10].

Один из принципиально новых методов И/А, не похожих на все предыдущие, был предложен в работе [11]. Суть предложенного метода – это И/А клиента на основе данных, собранных о нем. В ходе проведения И/А предлагается задавать клиенту вопросы, случайно созданные на основе имеющихся о нем данных. По результату полученных ответов – принимать решение об успешности процедуры И/А. Однако границы применимости этого подхода на практике неизвестны.

Цель данной работы – представить результаты имитационного моделирования системы И/А, использующей принципы описанного алгоритма. В дальнейшем в данной статье алгоритм, встроенный в моделируемую систему И/А, будем называть полифакторной аутентификацией.

I. Параметры имитационного моделирования

Предлагается рассмотреть модель системы И/А со встроенным алгоритмом полифакторной аутентификации (далее система полифакторной И/А) и ее функционирования на примере компании, в которой обслуживается 25 млн. клиентов ежедневно через дистанционные каналы, а максимальный поток клиентов в секунду – 40 тыс. человек. Обработка клиента в системе И/А должна происходить менее чем за $T_{\max} = 5$ мс для того, чтобы не ухудшать клиентский опыт (рис. 1).

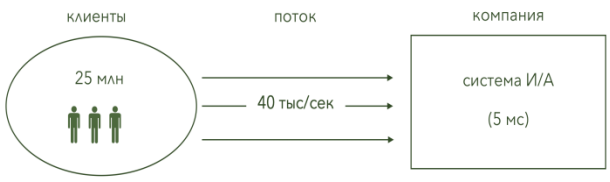

Рис. 1. Взаимодействие клиентов с компанией

Поскольку алгоритм полифакторной И/А использует информационные пространства (ИП) [11], описывающие поведенческие характеристики клиента, на основе которых будут формироваться аутентификационные вопросы, то необходимо их параметризировать. На каждого клиента создается матрица размером $r \times c$, где c – количество поведенческих характеристик клиента [12, 13]. Для примера, поведенческими характеристиками клиента могут быть: посещаемые магазины, страны путешествий, любимое кафе, потребляемые товары и т.д. Область определения (домен) каждого элемента матрицы – это случайные целые числа от 1 до d (рис. 2).

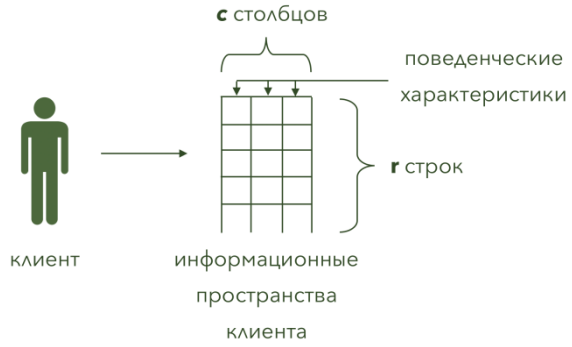

Рис. 2. Информационное пространство клиента

Кого-либо из клиентов возможно идентифицировать по одному вопросу, кого-то по двум и т.д. Поэтому введем распределение вероятностей идентифицировать клиента по 1-3 вопросам как параметры $\alpha_1, \alpha_2, \alpha_3$. Экспериментальным способом подтверждено, что параметр d влияет на распределение вероятностей $\alpha_1, \alpha_2, \alpha_3$: чем больше d, тем выше вероятность идентифицировать пользователя по одному вопросу, вместе с тем выше вероятность пользователя забыть ответ на вопрос в виду индивидуальной психический особенности такой, как глубина запоминания событий о себе. В данном моделировании не рассматриваются проблемы индивидуальных психических особенностей пользователя и принято следующее распределение вероятностей 0.85, 0.10, 0.05, полученное экспериментально.

A. *Алгоритм использования информационных пространств*

Каждая попытка И/А расходует 1, 2 или 3 строки в ИП клиента в зависимости от количества вопросов, определенных параметрами $\alpha_1, \alpha_2, \alpha_3$. При этом в ИП расходуются новые записи т.е. самые верхние строки матрицы, каждый раз, когда система И/А “задает” вопрос клиенту.

ИП пополняются “каждый” день на величину dv_1, т.е. количество строк в матрице увеличивается на dv_1. Также клиент может несколько раз в день проходить процедуру И/А, потребность клиента в процедуре И/А

определяется параметром dv_2 [14].

B. *Алгоритм расчета потока, вызывающего блокировку системы И/А*

Каждый запрос клиента к полифакторной системе И/А обрабатывается за время t_i, которое линейно зависит от (рис. 3):

- константы времени *dt*;
- количества строк в ИП клиента или *r*;
- количества вопросов, которые необходимо сформировать системе и задать клиенту в ходе процедуры И/А или *q*,

и рассчитывается по формуле $t_i = dt \cdot r \cdot q$.

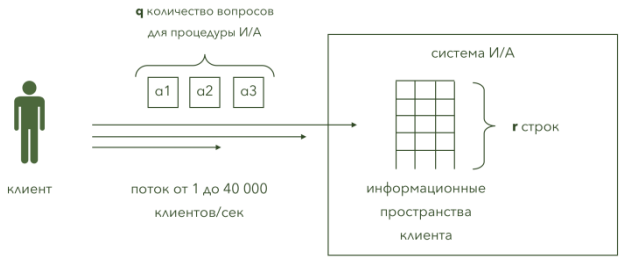

Рис. 3. Обработка запроса клиента полифакторной системой И/А.

Общее время, которое система И/А затратит на обработку потока в 40 000 клиентов/сек без распараллеливания, будет равно сумме времени обработки каждой индивидуальной сессии клиента с системой И/А или $T = \sum_{i=1}^{40000} t_i$.

Если общее время T на i-том шаге превысит порог $T_{\max}$ = 5мс, то каждый новый запрос клиента будет сохраняться в очередь и, следовательно, i-шаг и будет являться порогом, при котором блокируется обработка новых запросов клиентов.

C. *Задачи моделирования системы полифакторной И/А и ее функционирования*

Разработав модель системы И/А и ее функционирования, возникают следующие задачи:

(1) определение величины потока клиентов, который вызывает блокировку системы И/А (т.е. время отклика, превышающее 5 мс);

(2) определение минимального количества строк информационного пространства, при котором вероятность клиентов успешно пройти процедуру полифакторной И/А больше 0.9, а злоумышленника подобрать ответ меньше 0.05;

(3) определение доли клиентов, которые перестанут обслуживаться после 1 дня работы алгоритма по причине нехватки данных в информационных пространствах.

II. Описание алгоритма имитационного моделирования

Условно моделирование работы системы И/А возможно разделить на следующие 3 шага, выполняющихся последовательно.

A. ***Шаг 1.*** *Подготовка данных*

Генерация ИП (матриц) со случайным размером на каждого из 25 млн. клиентов предприятия. Каждый элемент матрицы – случайное целое число и принимает значение от 0 до *d* (рис. 4).

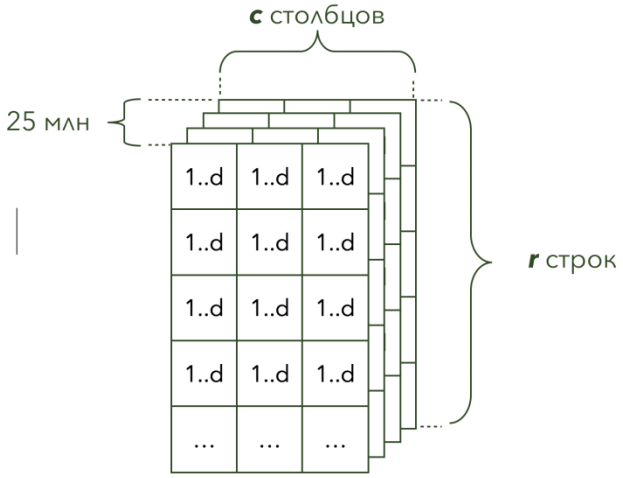

Рис. 4. Создание информационного пространства для каждого клиента

На основе созданных ИП алгоритм будет формировать случайные вопросы в отношении клиента. Случайный вопрос – это случайно выбранная строка в матрице (при моделировании использовались первые строки ИП).

B. ***Шаг 2.*** *"Рабочий день предприятия"*

Моделирование "рабочего дня предприятия", в течение которого предприятие обслуживает 25 млн. клиентов. Каждый из 25 млн. клиентов в течение дня проходит И/А по случайным вопросам. Количество вопросов, которые полифакторная система И/А "задает" клиенту определены распределением вероятности – $\alpha_1, \alpha_2, \alpha_3$. Результаты процедуры И/А каждого клиента можно описать следующим образом.

(1) Если в ИП клиента недостаточно данных, чтобы сформировать вопрос [15, 16], т.е. если количество строк в матрице клиента меньше количества вопросов, на которые ему необходимо ответить по процедуре И/А, то в таком случае необходимо зарегистрировать неуспешную попытку аутентификации, увеличив счетчик error на 1 единицу.

(2) Если в ИП клиента достаточно данных, чтобы сформировать вопрос, т.е. если количество строк в матрице клиента больше или ровно количеству вопросов, на которые ему необходимо ответить по процедуре И/А, то в таком случае, необходимо зарегистрировать успешную попытку аутентификации и удалить из матрицы данные, которые были использованы для формирования вопросов, увеличив счетчик success на 1 единицу.

Также возможен случай, когда клиент прошел успешно процедуру И/А, однако клиенту не хватит данных, чтобы пройти следующую процедуру И/А даже с учетом увеличения его информационного пространства на величину dv_1. В таком случае регистрируется предупреждение и счетчик warning увеличивается на 1 единицу.

Каждая процедура И/А клиента также оценивает возможность злоумышленника "угадать случайный вопрос". Понятно, что в реальной жизни злоумышленник не может начать угадывать вопросы, не обладая авторизованным устройством, не зная учетной записи жертвы и т.д. Тем не менее, разумно выполнить измерение данного показателя, чтобы оценить вероятность злоумышленника угадать правильный ответ. При каждой успешной попытке угадать случайный вопрос регистрируется попытка успешной атаки, и счетчик attack увеличивается на 1 единицу.

Шаг 2 возможно повторять несколько раз, изменяя какой-либо из параметров алгоритма, и наблюдая, как изменяются результаты. Повторяя данный шаг несколько раз, моделируется работа полифакторной системы И/А за несколько дней.

C. ***Шаг 3.*** *Подсчет результатов*

По результатам "прошедшего рабочего дня", т.е. после обработки полифакторной системой И/А 25 млн. клиентов, возможно рассчитать следующие показатели:

(1) оценку вероятности неуспешной попытки И/А или error по причине нехватки данных в информационных пространствах (ИП), которая измеряется отношением значения счетчика error к общему количеству клиентов, обслуживаемых за день, или $\frac{error}{25 \cdot 10^6}$, где *error* – число единиц в счетчике error;

(2) оценку вероятности успешной попытки И/А success, которая измеряется отношением значения счетчика success к общему количеству клиентов, обслуживаемых за день, или $\frac{success}{25 \cdot 10^6}$, где *success* – число единиц в счетчике success;

(3) оценку вероятности того, что для следующей попытки И/А не хватит данных в информационном пространстве или warning, которая измеряется отношением значения счетчика warning к общему количеству клиентов, обслуживаемых за день, или $\frac{warning}{25 \cdot 10^6}$, где *warning* – число единиц в счетчике warning;

(4) оценку вероятности злоумышленника "угадать" ответы на вопросы системы полифакторной аутентификации или attack, которая измеряется отношением значения счетчика attack к общему количеству клиентов, обслуживаемых за день, или $\frac{attack}{25 \cdot 10^6}$, где *attack* – число единиц в счетчике attack;

(5) мощность потока (клиенты/сек) при котором происходит блокировка системы т.е. время обработки нового запроса превышает $T_{\max} = 5$ мс.

III. Анализ полученных результатов имитационного моделирования

В результате моделирования работы системы полифакторной И/А получены следующие результаты.

(1) Время обработки запроса клиента зависит от потока (клиентов/сек.), количества строк в ИП клиента, количества вопросов, которые необходимо задать клиенту для прохождения процедуры И/А.

При потоке в 22 тыс. клиентов/сек. без распараллеливания происходит блокировка системы полифакторной И/А, начинает образовываться очередь из поступивших запросов, и время обработки каждого запроса составляет более $T_{\max} = 5$ мс. Таким образом не достигается одна из целей системы И/А по обработке потока в 40 тыс. клиентов/сек без образования очереди.

> При потоке в 22 тыс. клиентов/сек. без распараллеливания происходит блокировка системы полифакторной И/А.

Также наблюдаются локальные пики времени обработки, которые объясняются тем, что:

(а) попадаются клиенты с ИП, имеющими относительно большое число строк или *r*,

(б) системе И/А приходится формировать не 1, а 2 или 3 вопроса клиенту.

(2) Полифакторная И/А зависит от количества данных в информационных пространствах:

(а) при условии достаточности данных и условия отсутствия блокировки работы системы полифакторной И/А, оценка вероятности пройти успешную И/А клиентом близка к 1, а оценка вероятности подобрать ответ на вопрос полифакторной системы И/А злоумышленником меньше 0.05,

> Количество строк в ИП более (r>7) является оптимальным параметром алгоритма полифакторной И/А.

(b) минимальный "разумный" размер ИП составляет 7 строк,

(c) минимальный размер ИП, при котором возможно применить полифакторную И/А, составляет 4 строки.

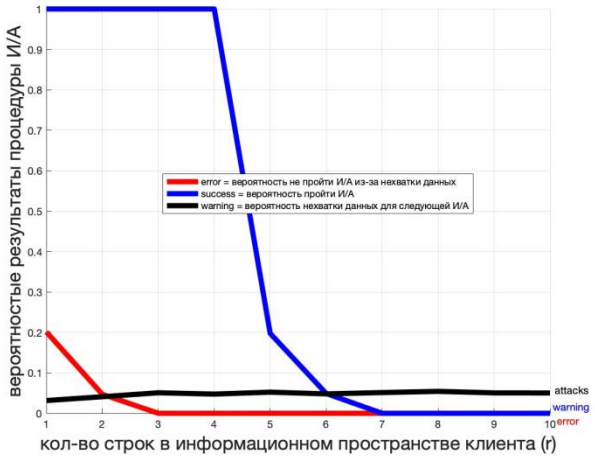

Рис. 5 Графики оценок вероятностей системы И/А

(3) Оценка вероятности успешной процедуры И/А (success) зависит от множества параметров: количества данных в ИП (r), мощности элементов ИП (d), величины потока и т.д.

На графике (рис. 6) представлена зависимость оценки вероятности успешной процедуры И/А (success) от количества данных в ИП (r) и мощности элементов ИП (d). При этом зависимость оценки вероятности успешной процедуры И/А от размера ИП (r) – нелинейная, а от мощности элементов ИП (d) – линейная.

Также, чем больше параметр d, тем больше оценка вероятности, что клиент забудет это событие. Однако в данной работе не рассматривались индивидуальные психические особенности клиентов.

Мощность элемента в ИП d>5 – оптимальный параметр алгоритма полифакторной И/А.

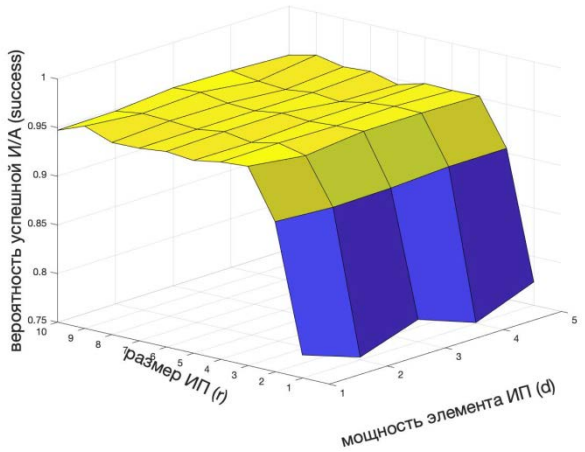

Рис. 6. График зависимости оценки вероятности успешной И/А (success) от размера ИТ и мощности множества элементов ИП

(4) Вероятность неуспешной процедуры И/А (error) зависит от множества параметров: количества данных в ИП (r), мощности элементов ИП (d), величины потока и т.д.

На графике (рис. 7) представлена зависимость оценки вероятности неуспешной процедуры И/А (error) от количества данных в ИП (r) и мощности множества элементов ИП (d). При этом зависимость оценки вероятности неуспешной процедуры И/А (error) от размера ИП (r) – нелинейная, а от мощности множества элементов ИП (d) – линейная.

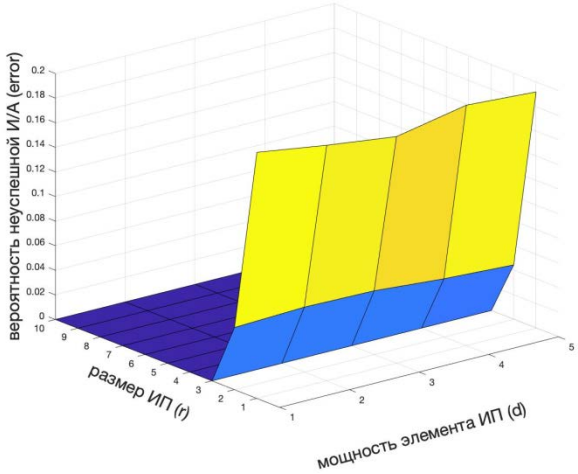

Рис. 7. График зависимости оценки вероятности неуспешной И/А (error) от размера ИП и мощности множества элементов ИП

(5) Оценка вероятности следующий раз неуспешно пройти процедуру И/А (warning) зависит от множества парамeнтов: количества данных в ИП (r), мощности множества элементов ИП (d), величины потока и т.д.

На графике (рис. 8) представлена зависимость оценки вероятности в следующий раз неуспешно пройти процедуру И/А (warning) от количества данных в ИП (r) и мощности множемтва элементов ИП (d). При этом зависимость вероятности неуспешной процедуры И/А (error) от размера ИП (r) – нелинейная, а от мощности множества элементов ИП (d) – линейная.

Также, если размер ИП (r) меньше или равен 3, то вероятность не пройти процедуру И/А (warning) равна 1, т.е. получаем запрет на последующую процедуру прохождения И/А. Понятие заапрета исследовалось, например, в работе [17].

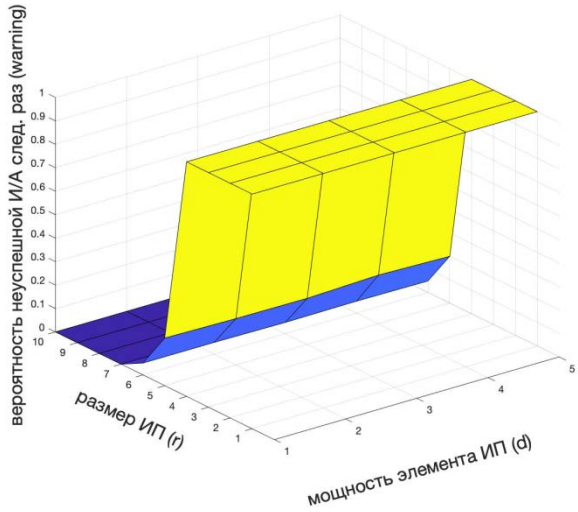

Рис. 8. График зависимости оценки вероятности не пройти следующий раз И/А (warning) от размера ИТ и мощности множества элементов ИП

(6) Оценка вероятности успешной атаки на процедуру И/А (attack) зависит от множества

параметров: количества данных в ИП (*r*), мощности множества элементов ИП (*d*), величины потока и т.д.

На графике (рис. 9) представлена зависимость оценки вероятности успешной атаки на процедуру И/А (attack) от количества данных в ИП (*r*) и мощности элементов ИП (*d*).

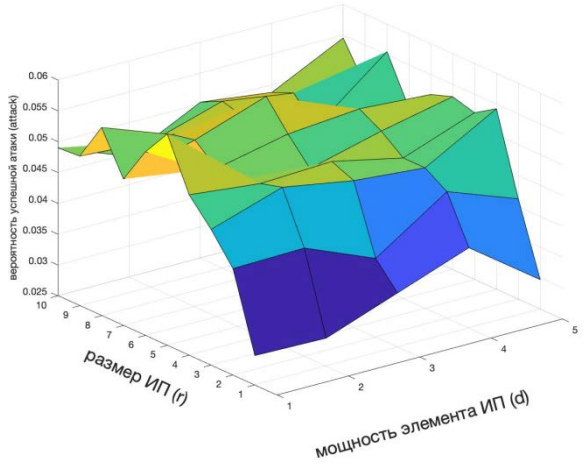

Рис. 9. График зависимости успешной атаки на систему И/А от размера ИП и мощности ИП

(7) Если величина расходования ИП dv_2 равна 2, то оценка вероятности успешной И/А, более или равной 0.9, будет при количестве строк r>6. Если величина расходования ИП dv_2 равна 3, то оценка вероятности успешной И/А, более или равной 0.9, будет при количестве строк r>10.

Рис. 10. Графики зависимости оценки вероятности успешной И/А (success) от расходования ИП или dv(2)

IV. Заключение

В выполненном моделировании не рассматривались индивидуальные психические особенности клиентов такие, как глубина запоминания событий о себе, лингвистическая корректность вопросов, которые полифакторная система И/А задает клиенту и т.д.

Параметры, используемые при имитационном моделировании и влияющие на процедуру И/А клиента, возможно разделить на две категории.

(1) Параметры, влияющие на алгоритм полифакторной И/А:

- количество строк в ИП (*r*),
- величина мощности элемента ИП (*d*),
- величина пополнения ИП dv_1,
- величина расходования ИП dv_2,
- количество вопросов, определенных параметрами $\alpha_1, \alpha_2, \alpha_3$.

(2) Параметры, влияющие на информационную систему, реализующую алгоритм И/А,:

- величина *потока*.

В ходе имитационного моделирования определены оптимальные значения параметров работоспособности алгоритма полифакторной И/А: r = 7, d = 5. Параметры dv_1, dv_2, $\alpha_1, \alpha_2, \alpha_3$ влияют на r и d.

При оптимальных параметрах r и d оценка вероятности подобрать ответ на вопрос полифакторной системы И/А злоумышленником близка к нулю, а оценка вероятности успешно пройти И/А клиентом близка к 1.

(3) Максимальная величина потока, которая способна обработать информационная система со встроенным алгоритмом полифакторной И/А – 22 тыс. клиентов/сек. Превышение указанной величины приводит к блокировке системы. Система требует распараллеливания, иначе требуемый уровень 40 тыс. клиентов/сек достигнуть невозможно.

Библиография

[1] И. Беров, “ЕБС набирает высоту”, *BIS Journal*, № 4(31), 29 декабря 2018, Available: https://journal.ib-bank.ru/post/776

[2] A.K. Nag, A. Roy, D. Dasgupta, “An adaptive approach towards the selection of multi-factor authentication,” *IEEE symposium series on computational intelligence*, 2015, pp. 463–472.

[3] M. Azimpourkivi, U. Topkara, B. Carbunar, “A Secure Mobile Authentication Alternative to Biometrics,” in *ACSAC 2017 Proc. of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 28-41, Available: https://arxiv.org/pdf/1712.02483.pdf.

[4] N. Micallef, N. A. G. Arachchilage, “Changing users’ security behaviour towards security questions: A game based learning approach,” in *Australasian Conference on Information Systems*, 2017, pp. 1-6. Available: https://arxiv.org/ftp/arxiv/papers/1709/1709.08623.pdf.

[5] U. Mahbub and R. Chellappa, "PATH: Person authentication using trace histories," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, 2016, pp. 1-8. Available: https://ieeexplore.ieee.org/document/7777911.

[6] F. Yao, S. Y. Yerima, B. Kang and S. Sezer, "Fuzzy logic-based implicit authentication for mobile access control," in *2016 SAI Computing Conference (SAI)*, London, 2016, pp. 968-975. Available: https://ieeexplore.ieee.org/document/7556097.

[7] Le Ngu Nguyen, Stephan Sigg, “Personalized Image-based User Authentication using Wearable Cameras,” Aalto University, 2016, pp.1-11. Available: https://arxiv.org/abs/1612.06209.

[8] F. Otterbein, T. Ohlendorf, M. Margraf, “The German eID as an Authentication Token on Android Devices,” 2017, Available: https://arxiv.org/ftp/arxiv/papers/1701/1701.04013.pdf.

[9] F. Yao, S. Y. Yerima, B. Kang and S. Sezer, "Event-Driven Implicit Authentication for Mobile Access Control," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, 2015, pp. 248-255, Available: https://ieeexplore.ieee.org/document/7373251.

[10] M. Portnoi and C. Shen, "Loc-Auth: Location-enabled authentication through attribute-based encryption," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, Garden Grove, CA, 2015, pp. 89-93, Available: https://ieeexplore.ieee.org/document/7069321.

[11] А. А. Грушо, М. И. Забежайло, Д. В. Смирнов, Е. Е. Тимонина, "О комплексной аутентификации," *Системы и средства информ*., Т. 27, Вып. 3, С.4–11, 2017.

[12] A. A. Grusho, N. A. Grusho, E. E. Timonina, "Content analysis in information flows," *AIP Conference Proceedings*vol. 1738, pp. 220002-1–220002-4, 2016.

[13] А. А. Грушо, Н. А. Грушо, М. И. Забежайло, Д. В. Смирнов, Е.Е. Тимонина, "Параметризация в прикладных задачах поиска эмпирических причин," *Информатика и ее применения*, Т. 12, № 3, С. 62-66, 2018.

[14] A. A. Grusho, E. E. Timonina, S. Y. Shorgin, "Modelling for ensuring information security of the distributed information systems," in Proc. of 31th European Conference on Modelling and Simulation, 2017, pp. 656-660.

[15] А. А. Грушо, Е. Е. Тимонина, "Запреты в дискретных вероятностно-статистических задачах," *Дискретная математика*, Т. 23, № 2, С. 53-58, 2011.

[16] А. А. Грушо, Н. А. Грушо, Е. Е. Тимонина, "Статистические методы определения запретов вероятностных мер на дискретных пространствах," *Информатика и ее применения*, Т. 7, № 1, С. 54-57, 2013.

[17] А. А. Грушо, М. И. Забежайло, А. А. Зацаринный, "Контроль и управление информационными потоками в облачной среде," *Информатика и ее применения*, Т. 9, № 4, С. 91-97, 2015.

Simulation Modeling of a Post-Biometric Method of Authentication on the Basis of User's Data

A. A. Grusho, M. I. Zabezhailo, D. V. Smirnov, E. E. Timonina

***Abstract* — Authentication data, such as password, key word, passport number, etc., authentication material, such as biometric fingerprint, faces, etc., authentication objects, such as phone, passport, token, etc., can be spotted, forged and transferred to the malefactor. The existing systems of multifactorial authentication are "finite-factor" systems, i.e. the quantity of factors used in authentication system and listed above is finite and in advance known. These vulnerabilities are used by hackers who constructed multichannel viruses with the help of which the computer and the smart phone of the victim are far away and hiddenly controlled at the same time. Controlling the smart phone of the victim, the hacker can hiddenly read SMS passwords or sometimes push-notifications. Thus, the four existing groups of authentication factors, such as cognitive, based on knowledge of the subject, biometric, based on physiology and behavior of the subject, the factors based on location of the subject and factors of possession of information or token have the following vulnerabilities:**

(1) the secret is separable from the user, and is on the client side,

(2) it is possible to repeat the password,

(3) it is possible to forge biometrics,

(4) the location can be arranged on conspiracy.

In the paper the new method of carrying out user authentication deprived of these vulnerabilities by means of the random questions created on the basis of the data which are available about the user is offered. The decision on success of the procedure of user authentication (polyfactor authentication) is being made on the base of results of his answers. The main problem of the offered method of authentication will be in finding optimum parameters of the authentication system implementing the offered algorithm and the algorithm implementing creation of questions. The purpose of research is to find such parameters.

***Keywords* — Information security, information spaces, simulation modeling, polyfactor authentication, parameters of algorithm.**

REFERENCES

[1] I. Berov, “EBS gains height”, *BIS Journal*, no. 4(31), 29 Dec. 2018, Available: https://journal.ib-bank.ru/post/776.

[2] A.K. Nag, A. Roy, D. Dasgupta, “An adaptive approach towards the selection of multi-factor authentication,” *IEEE symposium series on computational intelligence*, 2015, pp. 463–472.

[3] M. Azimpourkivi, U. Topkara, B. Carbunar, “A Secure Mobile Authentication Alternative to Biometrics,” in *ACSAC 2017 Proc. of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 28-41, Available: https://arxiv.org/pdf/1712.02483.pdf.

[4] N. Micallef, N. A. G. Arachchilage, “Changing users’ security behaviour towards security questions: A game based learning approach,” in *Australasian Conference on Information Systems*, 2017, pp. 1-6. Available: https://arxiv.org/ftp/arxiv/papers/1709/1709.08623.pdf.

[5] U. Mahbub and R. Chellappa, "PATH: Person authentication using trace histories," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, 2016, pp. 1-8. Available: https://ieeexplore.ieee.org/document/7777911.

[6] F. Yao, S. Y. Yerima, B. Kang and S. Sezer, "Fuzzy logic-based implicit authentication for mobile access control," in *2016 SAI Computing Conference (SAI)*, London, 2016, pp. 968-975. Available: https://ieeexplore.ieee.org/document/7556097.

[7] Le Ngu Nguyen, Stephan Sigg, “Personalized Image-based User Authentication using Wearable Cameras,” Aalto University, 2016, pp.1-11. Available: https://arxiv.org/abs/1612.06209.

[8] F. Otterbein, T. Ohlendorf, M. Margraf, “The German eID as an Authentication Token on Android Devices,” 2017, Available: https://arxiv.org/ftp/arxiv/papers/1701/1701.04013.pdf.

[9] F. Yao, S. Y. Yerima, B. Kang and S. Sezer, "Event-Driven Implicit Authentication for Mobile Access Control," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, 2015, pp. 248-255, Available: https://ieeexplore.ieee.org/document/7373251.

[10] M. Portnoi and C. Shen, "Loc-Auth: Location-enabled authentication through attribute-based encryption," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, Garden Grove, CA, 2015, pp. 89-93, Available: https://ieeexplore.ieee.org/document/7069321

[11] A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, D. V. Smirnov, E. E. Timonina, “About complex authentication,” *Systems and Means of Informatics*, vol. 27, no. 3, pp. 3-10, 2017.

[12] A. A. Grusho, N. A. Grusho, E. E. Timonina, “Content analysis in information flows,” *AIP Conference Proceedings*vol. 1738, pp. 220002-1–220002-4, 2016.

[13] A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, D. V. Smirnov, E. E. Timonina, “Parametrization in Applied Problems of Search of the Empirical Reasons,” *Informatics and Applications*, vol. 12, no. 3, pp. 62-66, 2018.

[14] A. A. Grusho, E. E. Timonina, S. Y. Shorgin, “Modelling for ensuring information security of the distributed information systems,” in Proc. of 31th European Conference on Modelling and Simulation, 2017, pp. 656-660.

[15] A. Grusho, E. Timonina, “Prohibitions in discrete probabilistic statistical problems,” *Discrete Mathematics and Applications*, vol. 21, no. 3, pp. 275-281, 2011.

[16] A. A. Grusho, N. A. Grusho, E. E. Timonina, “Statistical Methods of Definition of Bans of Probability Measures on Discrete Spaces,” *Informatics and Applications*, vol. 7, no. 1, pp. 54-57, 2013.

[17] A. A. Grusho, M. I. Zabezhailo, A. A. Zatsarinny, “Information flow monitoring and control in cloud computing environment,” Informatics and Applications, vol. 9, no. 4, pp. 95-101, 2015.