Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Кубанский государственный технологический университет»

На правах рукописи

Дзьобан Павел Игоревич

МЕТОДИКА И АЛГОРИТМЫ ЗАЩИТЫ АУТЕНТИФИКАЦИОННЫХ

ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В WEB - ПРИЛОЖЕНИЯХ

Специальность: 05.13.19 - Методы и системы защиты информации,

информационная безопасность

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель: кандидат технических наук, доцент А.В. Власенко

Краснодар - 2017

ОГЛАВЛЕНИЕ

1 ОБЗОР МЕТОДОВ И АЛГОРИТМОВ АУТЕНТИФИКАЦИИ

ПОЛЬЗОВАТЕЛЕЙ В WEB-ПРИЛОЖЕНИЯХ 17

1.1 Международный опыт создания защищенных web-приложений с учетом

актуальных атак злоумышленников 17

1.2 Методы обеспечения информационной безопасности аутентификации

пользователей в web-приложениях 20

1.3 Методы и алгоритмы аутентификации пользователей

в web-приложениях 23

1.3.1 Метод парольной аутентификации 24

1.3.2 Метод аутентификации по сертификатам 29

1.3.3 Метод аутентификации по одноразовым паролям 31

1.3.4 Метод аутентификации по ключам доступа 33

1.3.5 Метода аутентификации по токенам 34

1.4 Методы вторичной аутентификации 37

1.4.1 Метод генерирования одноразовых паролей 39

1.4.2 Метод табличной аутентификации 40

1.4.3 Метод с контрольными вопросами 43

1.4.4 Другие методы вторичной аутентификации 44

1.5 Международные и отечественные стандарты аутентификации 46

1.6 Выводы по первой главе 47

2 АНАЛИЗ АКТУАЛЬНЫХ ТИПОВ АТАК НА АУТЕНТИФИКАЦИОННЫЕ

ДАННЫЕ ПОЛЬЗОВАТЕЛЕЙ WEB-ПРИЛОЖЕНИЯ 48

2.1 Классификация атак на web-приложения 48

2.2 Примеры реализации атак на аутентификационные данные пользователей

web-приложения 53

2.2.1 Реализация сетевой атаки типа «фишинг» 54

2.2.2 Реализация сетевой атаки типа «Sql - инъекция» 55

2.2.3 Реализация сетевой атаки типа «ip-спуфинг» 56

2.3 Кеширование в web-браузере пользователей, как канал утечки

аутентификационных данных 57

2.4 Анализ SSL/TLS шифрования 59

2.4.1 Реализация дешифрования аутентификационных данных SSL/TLS шифрования 65

2.5 Выводы по второй главе 67

3 ИСПОЛЬЗОВАНИЕ БАЙЕСОВСКОЙ СЕТИ ДЛЯ ЗАЩИТЫ

КЛИЕНТСКОЙ СТОРОНЫ ОТ АТАК ЗЛОУМЫШЛЕННИКОВ 69

3.1 Существующие методы защиты от атак злоумышленников на стороне

клиента web-приложения 71

3.2 Описание математической модели байесовской сети 74

3.3 Байесовская математическая модель обнаружения и предотвращения

хищения аутентификационных данных пользователя web-приложения 78

3.4 Алгоритм реализации математической модели 89

3.5 Оценка эффективности предавторизационной проверки пользователей

web-приложений 92

3.6 Выводы по третьей главе 98

4 РАЗРАБОТКА МЕТОДИКИ И АЛГОРИТМОВ ЗАЩИТЫ

АУТЕНТИФИКАЦИОННЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В WEB-

ПРИЛОЖЕНИИ 100

4.1 Разработка методики и алгоритмов защиты аутентификационных данных

пользователей на стороне web-ресурса 100

4.2 Анализ и моделирование действий злоумышленника на возможность

хищения аутентификационных данных пользователей в результате атаки на сервер web-приложения 114

4.2.1 Использование метода радужных таблиц 114

4.2.2 Использование метода «грубого перебора» 115

4.2.3 Использование логирования для дешифровки аутентификационных

данных 116

4.3 Нагрузочное тестирование авторизационными данными сервера web-

приложения 117

4.4 Тестирование производительности многоканальной системой массового

обслуживания с неограниченной очередью авторизаций пользователей 121

4.5 Выводы по четвертой главе 127

5 ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДИКИ И АЛГОРИТМОВ ЗАЩИТЫ

АУТЕНТИФИКАЦИОННЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ WEB-

ПРИЛОЖЕНИЯ 129

5.1 Расчет возникновения риска реализации актуальных сетевых атак на

аутентификационные данные пользователей web-приложения 129

5.2 Влияние методики и алгоритмов защиты аутентификационных данных

пользователей web-приложения на информационные риски предприятия в целом 141

5.3 Выводы по пятой главе 143

ЗАКЛЮЧЕНИЕ 145

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ 147

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ 148

ПРИЛОЖЕНИЕ А 161

Листинг скрипта аутентификации для web-приложения c использованием

Php 161

ПРИЛОЖЕНИЕ Б 164

Листинг кода PHP базы данных web-приложения 164

ПРИЛОЖЕНИЕ В 165

Листинг кода Php для хеширования пароля 165

ПРИЛОЖЕНИЕ Г 167

Листинг реализации усиленной методики и алгоритмов защиты

аутентификационных данных пользователей web-приложения

с модификатором «соль» 167

ПРИЛОЖЕНИЕ Д 168

Свидетельство о государственной регистрации базы данных 168

ПРИЛОЖЕНИЕ Е 169

Свидетельство о государственной регистрации базы данных 169

ПРИЛОЖЕНИЕ Ж 170

Свидетельство о государственной регистрации базы данных 170

ПРИЛОЖЕНИЕ З 171

Акт о внедрении результатов диссертационной работы 171

ПРИЛОЖЕНИЕ И 172

Акт о внедрении результатов диссертационной работы 172

ПРИЛОЖЕНИЕ К 173

Акт о внедрении результатов диссертационной работы

ЗАКЛЮЧЕНИЕ

В диссертационной работе проведены исследования, обеспечивающие повышение целостности, конфиденциальности и доступности, входных иден-тификационных и аутентификационных данных пользователей на этапе вво¬да, передачи, обработки и хранения данных на web-сервере. В рамках дис¬сертационной работы получены следующие научные и практические резуль¬таты:

- произведен анализ предметной области, изучены существующие ме¬тодики и алгоритмы идентификации и аутентификации пользователей. Выяв¬лены преимущества и недостатки актуальных методик аутентификации поль¬зователей с точки зрения информационной безопасности; выявлено две про¬блемы: не реализован мониторинг web-ресурсов в реальном времени на на¬личие сетевых угроз, на стороне пользователя web-приложения; после де¬шифровки аутентификационных данных на сервере они поступают в СУБД для сравнения и дальнейшей аутентификации в открытом виде или с возмож¬ностью дешифрования, что ставит под угрозу контент не только данного ре¬сурса, но и остальных, где пользователь зарегистрирован - так как связки ключей в 95 % случаев совпадают;

- разработан и реализован алгоритм предавторизационной проверки web-приложения с использованием математической модели байесовской сети для расчета вероятности наступления угрозы сетевого типа в режиме реаль¬ного времени по 17 взаимосвязанным критериям и свойствам, тем самым предотвращается факт наступления сетевой угрозы на стороне пользователя и сервера web-приложения соответственно;

- разработаны и реализованы методика и алгоритмы защиты аутентификационных данных пользователей в web-приложении с использованием криптографического синтеза пароля, n-разового хеширования, с имитацией скомпрометированного коллизиообладаюшего шифрования, оригинального энтропийного модификатора «соль», зависимой от уникального ярлыка каждого пользователя. В базе данных web- приложения, для прохождения процедуры аутентификации, хранятся и сравниваются результаты хеш-суммы от синтеза идентификационных, аутентифкационных данных, ip-адреса и уникальной для каждого пользователя «соли»;

- разработан и реализован алгоритм многоканальной системы массо¬вого обслуживания с неограниченной очередью аутентификации пользовате¬лей web-приложения с учетом специфики авторской методики для определе¬ния пропускного и вычислительного ресурса информационной системы, в ко¬торой предполагается реализация разработанной методики;

- произведена оценка эффективности методики и алгоритмов защиты аутентификационных данных пользователей web-приложения, разработана частная модель угроз и нарушителя, процедуры аутентификации пользовате¬лей в web-приложении; следует отметить снижение риска на величину до 83 % по трем основным показателям (конфиденциальность, целостность, доступность) реализации сетевых угроз для процедур идентификации и ау¬тентификации пользователей в результате реализации предавторизационной проверки web-приложения на стороне пользователя и реализация n-го хеши¬рования с инструментами «сдвига» регистра и символьной «замены», разбав¬ленных модификатором «соль» для повышения криптостойкости, аутентифи¬кационных данных для сравнения хеш-сумм на сервере web-приложения;

- для выявления эффекта от внедрения авторской методики и алгорит¬мов защиты аутентификационных данных пользователей была рассмотрена организация компьютеризированных бизнес-процессов управления информа¬ционными рисками предприятия КБ «Кубань Кредит» ООО. Рассчитана и по¬лучена реальная экономическая эффективность от внедрения авторской мето¬дики и алгоритмов защиты аутентификационных данных пользователей в КБ «Кубань Кредит» ООО, выраженная в снижении ежемесячного возможност- ного ущерба от возникновения информационных рисков на 1,211 млн руб.

Проведенные исследования в области защиты аутентификационных данных пользователей web-приложения помогут значительно увеличить по¬казатель целостности и конфиденциальности входных данных пользователей и их дальнейшей аутентификации.