Практическая работа № 14

ИССЛЕДОВАНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ КОМБИНИРОВАННЫХ СРЕДСТВ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ

Цель работы. Изучить принципы комбинированной аутентификации субъектов и оценить их эффективность.

Краткие сведения из теории

Принципы, повышающие стойкость парольных методов опознания

Эффективность средств аутентификации определяется вероятностью подбора аутентификатора с первой попытки. Для повышения эффективности этих средств при их проектировании необходимо использовать следующие **принципы**:

- максимального правдоподобия;
- ограничения попыток;
- цикличности.

Принцип максимального правдоподобия заключается в следующем. Пусть $A = \{a_i\}$, $i = 1, n$ – эталонные значения параметров, используемых для аутентификации, а $X = \{x_i\}$, $i = 1, n$ – значения параметров, предъявляемых для опознания.

Пусть независимые попытки опознания имеют частные вероятности $\rho(X, A)$, тогда принцип максимального правдоподобия состоит в выборе в качестве истинного такого параметра X, при котором максимизируется функция правдоподобия:

$$L(\theta) = \rho(x_1, a_1), \rho(x_2, a_2), \ \ldots, \ \rho(x_n, a_n) . \qquad (1)$$

Для средств опознания, основанных на том, «что знает субъект» и «что имеет субъект», принцип максимального правдоподобия заключается в том, что опознание считается успешным при абсолютном совпадении всех сравниваемых признаков входного воздействия, предоставленного субъектом, и эталонного, хранящегося в памяти средства опознания. Это обусловлено тем, что результат преобразования признаков, предоставляемых одним и тем же субъектом, в понятный средству опознания вид всегда имеет одинаковые значения.

В этом случае *вероятность подбора пароля с первой попытки*

$$P_{\text{па1}} = \frac{1}{N}, \tag{2}$$

где N – объем алфавита.

Для паролей *объем алфавита*

$$N = A^n, \tag{3}$$

где A – используемый алфавит пароля (общее число знаков);

n – длина пароля.

Тогда

$$P_{\text{па1}} = \frac{1}{A^n}. \tag{4}$$

В средствах опознания с использованием смарт-карт субъект предоставляет PIN-код, состоящий из цифр. Поэтому алфавит PIN-кода равен десяти. Для этих средств опознания *формула определения вероятности подбора PIN-кода с первой попытки* имеет следующий вид

$$P_{\text{па1}} = \frac{1}{10^n}. \tag{5}$$

В средствах опознания с использованием электронных ключей или брелоков используются битовые ключи, поэтому алфавит ключей равен двум. *Формула определения вероятности подбора битового ключа с первой попытки* имеет вид

$$P_{\text{па1}} = \frac{1}{2^n}. \tag{6}$$

Вероятность подбора пароля с первой попытки при неповторяющихся символах в пароле

$$P_{\text{па1неповт}} = \prod_{i=0}^{n-1} \frac{1}{N-i}. \tag{7}$$

В данном случае количество символов не может быть больше алфавита.

Увеличение вероятности правильного опознания субъекта для данных средств аутентификации достигается за счет расширения алфавита или длины аутентификатора.

Для биометрических средств аутентификации абсолютное совпадение всех сравниваемых признаков входного воздействия и эталонного недостижимо. Это обусловлено тем, что процесс преобразования признаков, предоставленных субъектом, в понятный средству аутентификации вид носит

вероятностный характер. В этом случае принцип максимизации правдоподобия заключается в том, что аутентификация считается установленной, если величина несовпадения всех сравниваемых признаков входного воздействия, предоставленного субъектом, и эталонного, хранящегося в памяти средства аутентификации, не превышает некоторого значения меры близости сравниваемых признаков.

Увеличение вероятности правильного опознания субъекта для биометрических средств аутентификации достигается за счет минимизации значения меры близости сравниваемых признаков, что, с другой стороны, может привести к увеличению вероятности блокировки «своих» субъектов. Другим путем увеличения вероятности правильного опознания является максимизация алфавита биометрических признаков за счет изменения точности их получения и сравнения с эталонными. Например, для средства аутентификации по отпечатку пальца максимизацию алфавита биометрических признаков проводят за счет увеличения разрешения картинки отпечатка пальца, а для средства аутентификации по голосу – за счёт увеличения размера секторов, в которых происходит определение типа минуций.

Принцип ограничения попыток заключается в том, что при опознании субъекта ограничивается число попыток неправильного входа в систему. При *отсутствии ограничения* на число попыток неправильного входа значение вероятности подбора пароля определяется по формуле

$$P_{\text{па}} = P_{\text{па}1} + (1 - P_{\text{па}1})P_{\text{па}2} + (1 - P_{\text{па}1})(1 - P_{\text{па}2})P_{\text{па}3} + \\ + \cdots + (1 - P_{\text{па}1}) \times \cdots \times (1 - P_{\text{па}n\text{-}1})P_{\text{па}n}, \qquad (8)$$

где $P_{\text{па}i}$ – вероятность подбора пароля при наборе i-й комбинации с учетом того, что $i - 1$ комбинаций уже опробовано и нет смысла набирать их заново;

$$P_{\text{па}i} = \frac{1}{n - i + 1}, i = 1, 2, ..., n .$$

Подставив в формулу (8) выражения для $P_{\text{па}i}$, получим

$$P_{\text{па}} = \frac{1}{n} + \left(1-\frac{1}{n}\right)\frac{1}{n-1} + \left(1-\frac{1}{n}\right)\left(1-\frac{1}{n-1}\right)\frac{1}{n-2} + \cdots$$
$$+ \left(1-\frac{1}{n}\right)\times\cdots\times\left(1-\frac{1}{n-n+2}\right)\frac{1}{n-n+1} = \frac{1}{n} + \frac{n-1}{n}\frac{1}{n-1} +$$
$$+ \frac{n-1}{n}\frac{n-2}{n-1}\frac{1}{n-2} + \cdots + \frac{n-1}{n}\times\cdots\times\frac{n-n+1}{n-n+2}\frac{1}{n-n+1} =$$
$$= \frac{1}{n} + \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = n\frac{1}{n} = 1.$$

При использовании принципа ограничения попыток *вероятность подбора пароля за k попыток*

$$P_{\text{па}} = \frac{1}{n} + \left(1-\frac{1}{n}\right)\frac{1}{n-1} + \cdots + \left(1-\frac{1}{n}\right)\times\cdots\times\left(1-\frac{1}{n-k+2}\right)\frac{1}{n-k+1} = \frac{k}{n}, \quad (9)$$

где k – допустимое количество попыток неправильного входа в систему.

Вероятность подбора пароля за k попыток означает, что пароль будет подобран с первой или со второй, или … с k-й попытки. Поэтому в формулах (8) и (9) каждое слагаемое является вероятностью подбора пароля с определенной попытки.

Таким образом, *вероятность подбора пароля с i-й попытки*

$$P_{\text{сп}} = (1-P_{\text{па1}})(1-P_{\text{па2}})\times\cdots\times(1-P_{\text{па}i\text{-}1})P_{\text{па}i}. \quad (10)$$

Подставив в формулу (17) выражения для $P_{\text{па}i}$, получим

$$P_{\text{сп}} = \left(1-\frac{1}{n}\right)\left(1-\frac{1}{n-1}\right)\times\cdots\times\left(1-\frac{1}{n-i+2}\right)\frac{1}{n-i+1} = \frac{1}{n}. \quad (11)$$

Реализация данного принципа заключается в блокировке средства аутентификации при превышении допустимого количества попыток неправильного входа в систему.

Принцип ц и к л и ч н о с т и заключается в том, что средство опознания функционирует по заранее установленному жесткому циклу, и ни при каких входных воздействиях цикл его работы не нарушается.

При использовании данного принципа в качестве параметра, учет которого позволяет повысить эффективность средства опознания, выступает безопасное время действия пароля, связанное с вероятностью его подбора простым соотношением

$$T_{\text{без}} = \frac{P_{\text{т}}}{P_1}T_{\text{ц}} = NP_{\text{т}}T_{\text{ц}}, \quad (12)$$

где $T_{\text{без}}$ – безопасное время действия пароля;

$P_т$ – вероятность подбора пароля за время $T_{без}$;

$T_ц$ – время выполнения средством опознания одного цикла работы.

В силу того, что цикл работы жестко фиксирован, путем ввода некоторой временно́й задержки в конце цикла можно существенно повысить безопасное время действия пароля при постоянной вероятности подбора пароля. В данном случае *безопасное время действия пароля*

$$T_{без} = \frac{P_т}{P_1}(T_ц + t_з) = NP_т(T_ц + t_з), \quad (13)$$

где $t_з$ – временная задержка.

Отсюда

$$P_т = \frac{T_{без}}{N(T_ц + t_з)}. \quad (14)$$

Так как безопасное время действия пароля принято измерять, как минимум, в часах, а время выполнения средством опознания одного цикла работы и временной задержки – в секундах, то в формулу (14) следует ввести коэффициент, переводящий безопасное время действия пароля в часы:

$$P_т = \frac{3600T_{без}}{N(T_ц + t_з)}. \quad (15)$$

В этом случае *вероятность подбора пароля за безопасное время его действия*

$$P_т = \frac{3600T_{без}}{A^n(T_ц + t_з)}. \quad (16)$$

При использовании PIN-кода формула (8) имеет следующий вид:

$$P_т = \frac{3600T_{без}}{10^n(T_ц + t_з)}, \quad (17)$$

а при использовании двоичного ключа –

$$P_т = \frac{3600T_{без}}{2^n(T_ц + t_з)}. \quad (18)$$

Во многих средствах опознания предусматривается возможность субъектам самим назначать себе пароли независимо друг от друга. В этом случае существует вероятность того, что у двух разных пользователей могут оказаться одинаковые пароли. Это приводит к тому, что средство опознания

при обращении к ней одного субъекта может принять его за другого. Поэтому такие системы опознания должны проверяться по критерию «парадокс дней рождения».

Математически парадокс дней рождений формируется следующим образом. Если $an^{-0,5}$ предметов выбирается с возвращением из некоторой совокупности размером n, то вероятность того, что два из них окажутся одинаковыми, составляет величину

$$P_{\text{д}} = 1 - e^{\left(-\frac{a^2}{2}\right)}. \qquad (19)$$

Практически это означает, что в случайно подобранной группе из 24 человек вероятность наличия двух лиц с одним и тем же днём рождения составляет величину порядка 0,5.

Если количество пользователей системы принять за d, то тогда

$$a = \frac{d}{A^{n/2}}. \qquad (20)$$

Подставив выражение (20) в выражение (19), получим

$$P_{\text{д}} = 1 - e^{\left(-\frac{d^2}{2A^n}\right)}. \qquad (21)$$

Порядок выполнения работы

1 Изучить краткие сведения из теории.

2 По первой цифре шифра необходимо выбрать один из алфавитов пароля (A), представленных в таблице 1.

Таблица 1

Первая цифра шифра	A	Первая цифра шифра	A
0	10	5	59
1	26	6	69
2	33	7	76
3	36	8	128
4	43	9	256

3 По предпоследней цифре шифра необходимо выбрать длину пароля (k), представленную в таблице 2.

Таблица 2

Предпоследняя цифра шифра	k	Предпоследняя цифра шифра	k
0	9	5	10
1	6	6	4
2	11	7	7

3	13	8	12
4	8	9	5

4 По последней цифре шифра необходимо выбрать вероятность подбора пароля (P), которые представлены в таблице 3.

Таблица 3

Последняя цифра шифра	P	Последняя цифра шифра	P
0	10^{-10}	5	10^{-9}
1	10^{-15}	6	10^{-13}
2	10^{-8}	7	10^{-11}
3	10^{-12}	8	10^{-16}
4	10^{-14}	9	10^{-7}

5 Определить вероятности подбора комбинированного пароля с первой попытки и за время T = 2 ч, если первая часть пароля является 16-байтной произвольной строкой из некоторого файла, а вторая часть пароля задается для алфавита пароля A и длине ключа k. Время ввода одного варианта каждой части комбинированного пароля t = 10 с.

6 Изучить методику оценки времени, необходимого для подбора пароля. Определить время подбора пароля, если алфавит пароля A, длина пароля k, время ввода одного символа пароля t' = 0,5 с, клавиатура блокируется:

а) после каждого набора пароля – на $t_б$ = 0 с;

б) после каждого набора пароля – на $t_б$ = 3 с;

в) после каждого десятого набора пароля – на $t_б$ = 5 с;

г) после первого набора пароля – на $t_б$ = 1 с, после второго – на $t_б$ = 2 с, после i-го – на $t_б = i$ с.

7 Произвести оценку необходимой длины пароля для удовлетворения требований, предъявляемых к системе опознания. Определить минимальную достаточную длину пароля, удовлетворяющую следующим параметрам: алфавит пароля A, время ввода одного символа пароля t' = 0,5 с, вероятность подбора пароля за время, отводимое на подбор пароля, $T_{без}$ = 92 дня, ($P_т$) не более P.

Примеры решения задач

Задача 1. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длиной k_1 = 8 из алфавита A_1 = 10 и длиной k_2 = 4 из алфавита A_2 = 20 при времени ввода первой части ключа t_1 = 2 с, а второй – t_2 = 1 с.

Решение. Вероятность подбора комбинированного пароля

$$P_т = P_{т1}P_{т2}.$$

Вероятность подбора пароля за безопасное время его действия

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}.$$

Тогда

$$P_{\text{т}} = \frac{3600 \cdot 8}{10^8 \cdot 2} \cdot \frac{3600 \cdot 8}{20^4 \cdot 1} = 14400 \cdot 10^{-8} \cdot 1800 \cdot 10^{-4} = 2{,}592 \cdot 10^{-5}.$$

Ответ: $P_{\text{т}} = 2{,}592 \cdot 10^{-5}$.

Задача 2. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время $T = 4000$ ч $P_{\text{т}} = 10^{-10}$; алфавит $A = 10$; время набора одного символа $t = 2$ с.

Решение. Вероятность подбора пароля за безопасное время его действия

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}.$$

Время выполнения средством опознания одного цикла работы в таком случае будет

$$T_{\text{ц}} = kt.$$

Тогда

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(kt + t_{\text{з}})}.$$

Отсюда при условии $t_{\text{з}} = 0$

$$kA^k \geq \frac{3600T}{P_{\text{т}}t}.$$

Подставив исходные данные, получим

$$k \cdot 10^k \geq \frac{3600 \cdot 4000}{10^{-10} \cdot 2}; k \cdot 10^k \geq 7{,}2 \cdot 10^{16}; k = 16.$$

Ответ: $k = 16$.

Задача 3. Определить время подбора пароля, состоящего из шести символов (k) из алфавита $A = 20$ при времени ввода одного символа $t = 3$ с.

Решение. Вероятность подбора пароля за безопасное время его действия

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}.$$

Отсюда, при условии, что $P_т = 1$, $T_ц = kt$ и $t_з = 0$,

$$T = \frac{A^k tk}{3600}.$$

Подставив исходные данные, получим

$$T = \frac{20^6 \cdot 3 \cdot 6}{3600} = 36{,}5 \text{ года}.$$

Ответ: $T = 36{,}5$ года.

Содержание отчета

1 Цель работы.
2 Исходные данные.
3 Результаты расчетов.
4 Вывод по работе.

Контрольные вопросы

1 Что такое идентификация субъекта?
2 Что такое аутентификация субъекта?
3 Классы средств аутентификации.
4 Как оценивается эффективность парольного средства аутентификации?.
5 Как оценить время жизни пароля?
6 Что такое комбинированные пароли?
7 Что такое «парадокс дня рождения»?