256-КАМ и схем с низкими скоростями кода при модуляции 4-ФМ. Результаты расчёта сведены в таблицу.

ТАБЛИЦА. Пропускная способность сети eMBMS LTE

Модуляция	$R_{код}$×1024	Сквозная скорость, Мбит/с			
		5 МГц	10 МГц	15 МГц	20 МГц
4-ФМ	602	1,79	3,59	5,39	7,19
16-КАМ	378	2,25	4,51	6,77	9,03
16-КАМ	490	2,92	5,85	8,78	11,7
16-КАМ	616	3,68	7,36	11,0	14,7
64-КАМ	466	4,17	8,35	12,5	16,7
64-КАМ	567	5,08	10,1	15,2	20,3
64-КАМ	666	5,97	11,9	17,9	23,8
64-КАМ	772	6,92	13,8	20,7	27,6
64-КАМ	873	7,82	15,6	23,4	31,3
64-КАМ	948	8,49	16,9	25,4	33,9

Скорость передачи видео в формате HDTV 720p (1280x720) с частотой 30 кадров в секунду с применением кодека H.264 составляет до 1 Мбит/с. Кодеки eMBMS не отличаются от кодеков для просмотра потокового видео в режиме одноадресного соединения с сервером. Из результата расчётов в таблице следует, что посредством технологии eMBMS можно обеспечить до 30 каналов высокой чёткости и в разы больше каналов более низкого качества.

Список используемых источников

1. Волков А. Н., Рыжков А. Е., Сиверс М. А. UMTS – стандарт сотовой связи 3-го поколения. СПб.: Линк, 2008. 224 с. ISBN 5-98595-011-5.

2. Global Mobile Suppliers Association. URL: http://www.gsacom.com/

3. 3GPP TS 36.331 V12.7.0. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification. 2015. 453 p.

4. 3GPP TS 36.213 V12.7.0. Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures. 2015. 241 p.

ОБОБЩЕННАЯ МОДЕЛЬ НЕПОДСМАТРИВАЕМОГО ГРАФИЧЕСКОГО ПАРОЛЯ

В.В. Архипов, В.А. Яковлев

С самых общих позиций рассматривается задача построения неподсматриваемого пароля на основе использования таблицы соответствия вводных и парольных символов. Рассмотрены атаки на систему паролирования, получены соотношения для оценок вероятностей угадывания пароля и подбора пароля для различного числа возможных атак (подсматриваний) на процедуру ввода пароля.

Ключевые слова: аутентификация, паролирование, графический пароль, атака подсматривания, неподсматриваемый пароль.

THE GENERALIZED MODEL OF GRAPHICAL PASSWORD, TOLERANT TO VIDEO-RECORDING ATTACKS

Arkhipov V., Yakovlev V.

We tried to explain problem of producing password tolerant to video-recording attacks. This password based on a table of correspondences of input and password symbols. Attacks to system of password protection are considered, ratios for estimates of probabilities of guessing of the password and password guessing for different number of possible attacks to a password entry procedure are received.

Keywords: authentication, password protection, graphical password, video-recording attacks, Graphical password, tolerant to video-recording attacks, shoulder-surfing attacks

В последнее время большое внимание уделяется созданию систем аутентификации на основе паролей устойчивых к атакам «подсматривания» [1, 2, 3, 4, 5]. Предложено достаточно много неподсматриваемых графических паролей (НГП), некоторые из которых реализованы. Анализ этих парольных систем показывает, что они используют в своей основе принцип, состоящий в том, что пользователь при вводе пароля не указывает (не показывает) парольный символ (ПС), а использует некоторый другой символ из подмножества символов связанных с парольным символом. Назовем этот символ вводным (ВС). Подсматривание вводного символа не дает нарушителю однозначного ответа, какой парольный символ был введен.

В данной работе сделана попытка построения обобщенной модели НГП и приведены соотношения для оценки его стойкости к различным видам атак.

1. Модель НГП

Пусть $\tilde{P}$ – множество парольных символов (p_1, p_2, … , p_N) представляющих собой цифры, буквы, пиктограммы и пр. Символы, которые могут быть отображены на экране дисплея. $|\tilde{P}|$ – мощность этого множества.

Паролем PW назовем цепочку p_1, p_2, … p_N длиной N, составленную из символов $p_i \in \tilde{P}$. Пусть $\tilde{V}$ – множество символов ввода (цифры, буквы, пиктограммы и пр. символы), которые используются для ввода пароля и которые тоже могут быть отображены на дисплее. Мощность множества вводных символов $|\tilde{V}|$.

В обобщенном виде НГП можно пояснить с помощью таблицы ввода, которая может быть построена следующим образом.

Первая строка подмножества всех парольных символов $p_i \in \tilde{P}$, $i = 1, 2, \ldots N$.

Каждый столбец таблицы подмножество вводных символов V_{Pi}, соответствующих парольным символам p_i, т. е. $V_{Pi} = V_{1i}, V_{2i} \ldots V_{2K.}\ V_{iK} \in \tilde{V}$.

Назовем подмножество V_{Pi} блоком вводных символов. В общем случае количество символов K в блоке может быть разным.

Таблица строится таким образом, чтобы любой вводный символ V_{ij} повторялся в s_0 блоках.

Для аутентификации пользователя таблица выводится на экран дисплея. Пользователь, проходя аутентификацию, вместо парольного символа P_i выбирает любой символ v_{ij} из блока V_{pi}. Нарушитель, наблюдая за процедурой ввода, не может точно определить парольный символ, поскольку вводный символ встречается в s_0 блоках.

При вводе следующего парольного символа генерируется новая таблица ввода и процедура ввода повторяется.

Усиленным вариантом НГП на основе таблицы ввода может быть НГП, для которого на экране дисплея выводятся несколько таблиц ввода с различным заполнением символов $p_{ij} \in V_p$. Пользователь выбирает одну из таблиц, используя дополнительный парольный символ. При этом нарушитель не знает, какую таблицу использовал пользователь.

Примером таблиц, которые могут быть построены таким образом, являются пароль «Шахматы» [6] и BlackBerry [7].

Далее рассмотрим случай, когда для паролирования используется только одна таблица.

2. Атаки на НГП

Предположим, что нарушитель полностью знаком с принципом построения и параметрами таблицы ввода, знает подмножества $\tilde{P}$ и $\tilde{V}$ парольных и вводных символов. После каждого подсматривания нарушитель знает состав блоков вводных символов и символ ввода. Также будем предполагать, что после подсматривания нарушитель может делать одну попытку ввода пароля.

Атака угадывания. Нарушитель умозрительно угадывает символ пароля, на основе, имеющейся у него информации о подмножестве парольных символов после подсматривания.

Атака подбора. Нарушитель реализует попытку ввода парольного символа, используя таблицу ввода с учетом информации, получаемой в результате подсматривания. Заметим, что при атаке подбора аутентификация осуществляется без определения парольного символа.

Атака подсматривания. Сама атака подсматривания непосредственно не приводит к определению парольного символа. Нарушитель получает информацию о составе таблицы ввода и вводном символе, который использовал пользователь. Далее для аутентификации нарушитель должен использовать атаку угадывания или подбора.

Обозначим через $P^0_{\text{уг}}, P^0_{\text{подб}}$ – вероятности угадывания и подбора до атаки подсматривания, $P^i_{\text{уг}}, P^i_{\text{подб}}$ – эти же вероятности после i-ой атаки подсматривания.

3. Оценка вероятности угадывания

Пусть $\tilde{S}$ – любое подмножество блоков в ТВ, содержащих вводных символов $v \in \tilde{V}$, $\left|\tilde{S}\right| = s_0$ и пусть это условие выполняется для всех v.

Когда нарушитель 1-ый раз наблюдает за процедурой ввода, он видит вводный символ v и однозначно определяет s_0 блоков V_{p_i} и, соответственно, s_0 кандидатов в парольные символы $p_i, i = \{1,2,...,s_0\}$, из которых один парольный символ. Обозначим это подмножество $\tilde{S}_1$, $|\tilde{S}_1| = s_1$, $s_1 = s_0$

Если нарушитель наблюдает еще одну процедуру ввода, то он также получит s_0 кандидатов в парольные символы. Обозначим это подмножество $\tilde{S}_2'$.

В подмножествах $\tilde{S}_1$ и $\tilde{S}_2'$ есть хотя бы один общий символ (парольный символ). Обозначим через $s_2 = |S_1 \cap \tilde{S}_2'|$ количество кандидатов в парольные символы после второго подсматривания.

Аналогично можно записать:

$S_3 = S_2 \cap \tilde{S}_3' = S_1 \cap \tilde{S}_2' \cap \tilde{S}_3'$. Мощность этого подмножества $s_3 = |S_2 \cap \tilde{S}_3'|$.

В любом подмножестве $\tilde{S}_i'$ количество элементов s_0, однако, в подмножествах $\tilde{S}_i, i \geq 2$ количество элементов s_i случайное. Пусть S_i – случайная величина количества кандидатов в парольные символы в множестве $\tilde{S}_i$, $P(S_i = j)$ – вероятность того, что после i-го подсматривания в множестве $\tilde{S}_i$ будет j кандидатов в парольные символы. Тогда вероятность угадывания парольного символа $P_y^i(S_i = j) = \frac{1}{j}$. Усредняя по всем j, запишем:

$$P_y^i = \sum_{j=1}^{S_0} \frac{P(S_i)}{j}. \qquad (1)$$

Заметим, что после первого подсматривания $P(S_1 = s_0) = 1$, $P(S_1 = j) = 0$, $j < s_0$, поэтому $P_y^1 = \frac{1}{s_0}$.

Распределение вероятностей $P(S_i = j)$ для i-го подсматривания может быть получено из распределения вероятностей $P(S_{i-1})$ согласно следующему рекуррентному уравнению:

$$P(s_1 = s_0) = 1,$$

$$P(S_i = j) = \sum_{s \geq j}^{s^*} P(S_i = j / S_{i-1} = s) \cdot P(S_{i-1} = s),\ j \geq 2,$$

где s^* – максимальное значение s_{i-1}.

Для нахождения вероятности $P(S_i = j / S_{i-1} = s)$ переформулируем задачу нахождения количества символов в подмножестве $\tilde{S}_i = \tilde{S}_{i-1} \cap \tilde{S}_i'$ следующим образом.

Задано множество из N элементов. Из множества случайным образом выбирается (без возвращения) s_0 элементов. Выбранные элементы помечаются и

помещаются обратно в множество. Снова случайным образом выбирается s_0 элементов. Требуется найти вероятность того, что были вынуты ранее помеченные элементы в количестве $j = 0,1,..., s-1$. Учитывая тот факт, что парольный символ будет выпадать после каждого подсматривания, т.е. всегда будет выбран хотя бы один помеченный элемент, несложно получить следующее выражение:

$$P(S_i = j) = \frac{C_{s-1}^{j} \cdot C_{(N-1)-(s-1)}^{s_0-1-j}}{C_{N-1}^{s_0-1}}.$$

На рисунке 1 показаны зависимости $P(S_i = j)$ для значений $N = 10$, $s_0 = 5$.

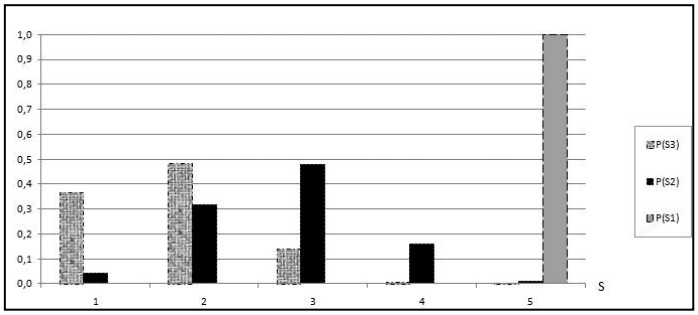

Рис. 1. Зависимости $P(S_i = j)$ для значений $N = 10$, $s_0 = 5$

На рисунке 2 показаны зависимости Py для значений $N = 10$, $s_0 = 5$.

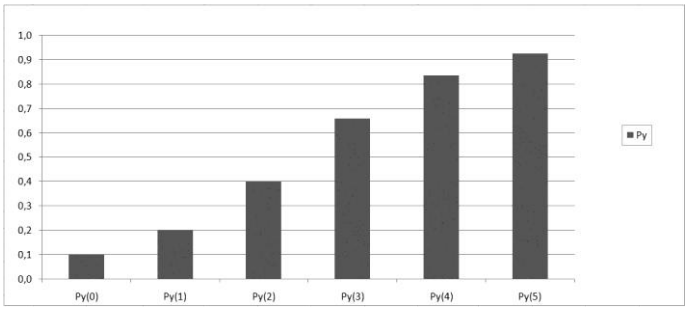

Рис. 2. Зависимости Py для значений $N = 10$, $s_0 = 5$

4. Оценка вероятности подбора

После проведения i-ой атаки подсматривания нарушитель знает s_i кандидатов в парольные символы $p_1, p_2, ... p_{Si}$.

Каждому такому символу в таблице ввода соответствует блок из K символов ввода. Причем один из блоков точно соответствует парольному символу. Поэтому стратегия нарушителя в i-ой атаке подбора может быть такой:

– начать процедуру аутентификации, вызвать на дисплей таблицу ввода;

– подсчитать количество совпадающих символов различного типа в s_i блоках;

– выбрать в качестве вводного символа тот, число повторений для которого в этих блоках максимально;

– если несколько символов максимальное количество повторений одинаково, то выбрать любой из них в качестве вводного символа.

Выражения для вероятности подбора можно записать так:

$$P^{i}_{\text{подб}} = \sum_{j=1}^{S_0} P(S_i = j) \cdot P_{\text{подб}}(S_i), \qquad (2)$$

где $P_{\text{подб}}(S_i)$ – вероятность подбора парольного символа при известном подмножестве $\tilde{S}_i$ кандидатов парольных символов после i-го подсматривания.

$$P_{\text{подб}}(S_i = j) = \sum_{m=1}^{N_t} \sum_{t=1}^{j} P_{conf}(m,t) \cdot \frac{t}{j},$$

где $P_{conf}(m,t)$ – вероятность m-ой конфигурации веса t; N_t – количество конфигураций веса t; $\frac{t}{j}$ – вероятность подбора для конфигурации веса t.

Под конфигурацией веса t мы понимаем расположение t блоков, среди j блоков, содержащих максимально повторяющийся вводный символ.

Аналитическое выражение для нахождения $P_{conf}(m,t)$ очень громоздко и зависит от способа построения таблицы ввода. Поэтому для вычисления $P_{conf}(m,t)$ будем использовать имитационное моделирование.

На рисунке 3 показаны зависимости $P^{i}_{\text{подб}}$, как функция от i согласно выражению (2), для N = 10, K = 5 для разного количества подсматриваний.

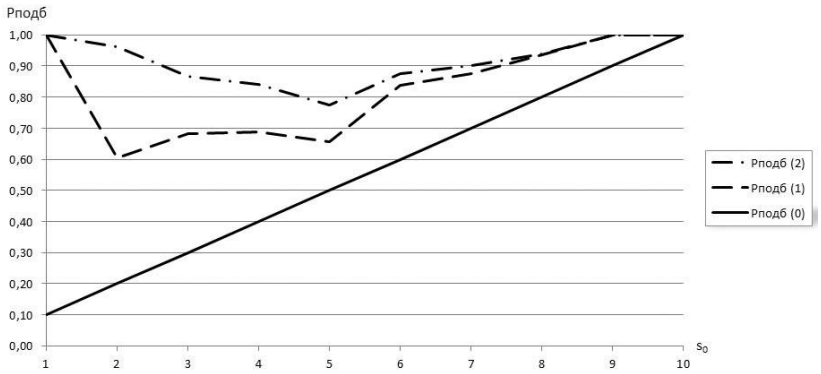

Рис. 3. Зависимости $P^{i}_{\text{подб}}$ для значений N = 10, K = 5

Заключение

В работе рассмотрены общие закономерности построения НГП, которые могут быть описаны в терминах набора таблиц ввода.

Полученные соотношения $P^{i}_{\text{угад}}$, $P^{i}_{\text{подб}}$ позволяют оценить защищенность достаточно большого количества типов НГП.

Список используемых источников

1. Sobrado L., Birget J.C. Graphical passwords // The Rutgers Scholar, vol. 4, 2003.

2. Luca A. D., Hertzschych K., Hussmann H. ColjrPIN: Securing PIN entry through indirect input // Proc. CHI, 2010, pp. 1103–1106.

3. Bianchi A., Oakley I., Kostakos V., Kwon D.-S. The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices // Proc. TEI, 2011, pp. 197–200.

4. Bianchi B., Oakley I., Kwon D.-S. Counting clicks and beeps: Exploring numerously based haptic and audio PIN entry. Interact. Comput., 2012, vo. 24, no. 5, pp. 409–412.

5. Яковлев В. А., Архипов В. В. Аутентификация пользователей на основе устойчивого к подсматриваниям графического пароля «Шахматы» // Проблемы информационной безопасности. Компьютерные системы. 2014. № 1. С 25–35.

6. Архипов В. В., Яковлев В. А. Способ аутентификации пользователей с защитой от подсматривания. Пат. 2541868 Российская Федерация; заявитель и патентообладатель ФГОБУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – № 2013122262/08; заявл.14.05.2013; опубл. 20.02.2015.

7. Kleidermacher D. Picture Perfect Privacy for PRIV. URL: http://blogs.blackberry.com/2015/12/picture-perfect-privacy-for-priv/. (дата обращения 08.12.15).

АНАЛИЗ НЕИСПРАВНОСТЕЙ В СЕТЯХ PON. ТЕОРИЯ И ПРАКТИКА

А.В. Астахов, В.Р. Сумкин

Практика поиска и устранения неисправностей при монтаже сетей PON показала, что наличие избыточного количества изгибов оптического волокна приводит к большим потерям на длине волны 1490 нм, тогда как недостаточно плотная фиксация оптических разъёмов существенно сильнее сказывается на затухании излучения на длине 1310 нм. Для объяснения этой особенности был проведён теоретический анализ потерь на макроизгибах оптического волокна и потерь на продольном зазоре для различных длин волн, используемых в сетях PON.

Ключевые слова: пассивная оптическая сеть, тестирование PON, оптическое волокно, спектральный диапазон, длина волны, оптическое излучение.

ANALYSIS OF TROUBLESHOOTING IN PON. THEORY AND PRACTICE

Astakhov A, Sumkin V.

As the practice of troubleshooting during the installation of PON shows, the presence of excess fiber bends causes the large losses at a wavelength of 1490 nm, whereas not enough tight fixations of optical connectors greatly affects the attenuation at a wavelength of 1310 nm. Theoretical analysis of losses caused by optical fiber macrobends and losses at a longitudinal gap for different wavelengths used in PON was carried out to explain this feature.

Keywords: passive optical network, PON testing, optical fiber, spectral range, wavelength, optical radiation

Тестирование распределительных сетей PON, выявление и устранение дефектов при строительстве и во время приемо-сдаточных работ являются важ-