Инженерный вестник Дона, №1 (2019)
ivdon.ru/ru/magazine/archive/n1y2019/5594

Повышение сложности пароля пользователя на основе комплексирования символов пароля и временных интервалов между ними

Д.В. Фатхи, В.В. Галушка

Донской государственный технический университет, Ростов-на-Дону

Аннотация: Статья посвящена актуальной проблеме повышения сложности пользовательских паролей в системах с удалённым доступом для повышения их информационной безопасности. В ней предлагается метод, основанный на комплексном применении вводимых символов пароля и временных промежутков между ними. В статье с помощью ингибиторной временной сети Петри построена модель динамического процесса задания пароля, на её основе описан процесс формирования эталонного образа и аутентификации пользователя. Приводимые расчёты повышения сложности пароля доказывают эффективность предлагаемого подхода.
Ключевые слова: аутентификация, пароль, динамический процесс, сеть Петри, сложность, подбор пароля полным перебором.

Введение

Среди известных на сегодняшний день методов аутентификации, наиболее распространённым и простым является использование паролей [1], однако, данный метод обладает большим количеством недостатков. Зачастую пользователи устанавливают простые пароли, которые легко угадать; пароль также может быть перехвачен при вводе. Помимо паролей, в некоторых системах, аутентификацию пользователей проводят также по одному из следующих видов представления информации [2]: предмету с уникальными характеристиками или уникальным содержанием, например, смарт-карта или usb-ключ; отпечаткам пальцев или биометрической информации.

Каждый из перечисленных видов представления имеет свои недостатки, для устранения которых, часто применяют комбинации различных способов аутентификации [3], например, двухфакторная аутентификация с использованием смарт-карты и PIN-код или пароля и подтверждения из смс-сообщения, что повышает безопасность, но и значительно затрудняет саму процедуру аутентификации, добавляя в неё

этапы с возможностями для совершения ошибок и потенциальными уязвимостями [4]. В связи с этим актуальной является задача построения сильной системы аутентификации с удобным и простым применением паролей, неуязвимых для словарных атак и других вариантов подбора, с целью повышения сложности раскрытия парольной аутентификации. Её достижение возможно путём комплексирования символьной части паролей и задаваемых пользователем временных интервалов между вводимыми символами в качестве информационной составляющей.

Процесс аутентификации

Пользователь, пытающийся получить удаленный доступ к сетевому сервису, проходит аутентификацию на компьютере, реализующем программные средства, которые, формируют пароль-эталонный образ пользователя и выполняют его сравнение с вводимыми данными. Пароль запрашивается дважды и хранится в таблице соответствий «пользователь-эталон» в зашифрованном виде или в виде хэша, что не позволяет злоумышленнику, получившему доступ к хранилищу эталонов, ознакомиться с учётными данными всех пользователей системы [5].

Когда пользователь проходит аутентификацию, у него запрашивается аутентификационная информация, и на основании её сравнения с эталоном пользователь считается опознанным или нет.

Рассмотрим кортеж $A_{\text{п}}$, представляющий собой пароль, сформированный по рассматриваемому методу и содержащий символы и временны́е интервалы между ними. Данный кортеж имеет вид:

$$A_{\text{п}} = (S_1, T_1, S_2, T_2, \ldots, T_{n\text{-}1}, S_n), \quad (1)$$

где S_i — символы пароля, $i = 1, 2, \ldots, n$; T_j — интервалы времени между j и j–1 символом, $j = 1, 2, \ldots, n$–1; n — количество символов в пароле.

Символы S_i и T_j задаются пользователем и однозначно определяются им.

Необходимо отметить, что известен способ аутентификации по клавиатурному почерку [6, 7], в котором используются интервалы времени между символами, а кроме них, ещё количество опечаток, время удержания клавиш, число перекрытий между клавишами, скорость набора и степень его аритмичности. После статистической обработки этих данных рассчитываются эталонные характеристики пользователя, по которым его можно аутентифицировать только с определенной вероятностью. Особенность задачи аутентификации по этому способу состоит в необходимости обучения программы. Кроме того, аутентификация по клавиатурному почерку неприемлема для обеспечения высокого уровня защиты. В связи с этим необходимо разработать собственный алгоритм формирования и проверки паролей, учитывающий временные интервалы между вводом символов.

Модель динамического процесса формирования эталонного пароля и его проверки

Для реализации рассмотренных алгоритмов, при создании интервалов времени между символами пароля, применяется так называемое модельное время. Оно используется как при задании пароля в системе, так и при введении пароля в процессе аутентификации. Модельное время создается программной реализацией динамического процесса, обращаясь к которой можно фиксировать интервалы времени путём отсчёта минимальных отрезков. Сравнение эталонного интервала времени с интервалом времени при вводе пароля осуществляется повторным проведением процесса (сравниваемого) по последовательности выбранных в динамическом процессе минимальных отрезков (эталонного).

Рассмотрим динамические процессы, реализуемые в системе при задании пароля и при вводе пароля в виде сетевой модели на основе ингибиторной временной сети Петри [8]. На рисунке 1 представлена ингибиторная

временная сеть Петри [9], моделирующая динамические процессы, реализуемые в системе при задании пароля и при вводе пароля пользователем.

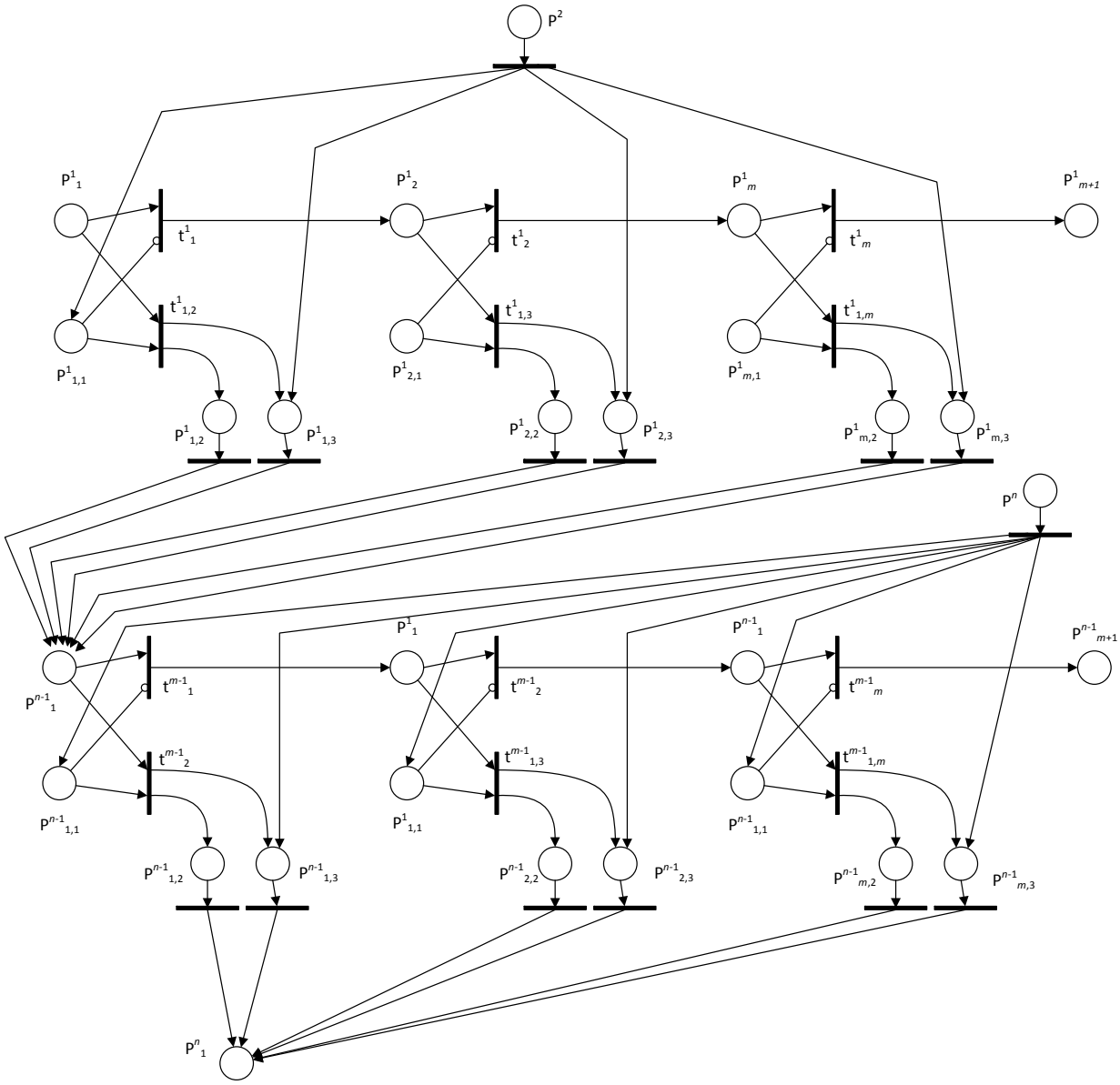

Рис. 1 – Ингибиторная временная сеть Петри, моделирующая динамические процессы, реализуемые в системе при задании пароля и при вводе пароля пользователем.

Рассмотрим задание пароля. В модели начало процесса инициируется меткой в позиции $P^1{}_1$, что соответствует заданию первого символа пароля путём нажатия кнопки [10]. Задаваемый символ обрабатывается

соответствующими программными средствами и сохраняется в качестве первого символа пароля. Метка из позиции P^1_1 через определенный интервал, формируемый моделью в качестве единицы измерения времени поступает в позицию P^1_2, затем в P^1_3 и так далее, и в конечном итоге — в P^1_m. В процессе перемещения метки, при задании второго символа (нажатии на выбранную пользователем кнопку клавиатуры), что соответствует появлению метки в позиции P^2 и переходу её в позиции $P^1_{1,1}$, P^1_{21}, …, $P^1_{m,1}$, срабатывают ингибиторные дуги, запирая переходы t^1_1, t^1_2, …, t^1_m. Движение метки останавливается, характеризуя значение интервала времени между нажатиями кнопок первого и второго символов пароля. Остановленная метка, находящаяся в одной из позиций $P^1_{1,1}$, P^1_{21}, …, $P^1_{m,1}$ через сработавший один из переходов $t^1_{1,2}$, $t^1_{1,3}$, …, $t^1_{1,m}$ переходит в одну из пар позиций $P^1_{1,2}$, $P^1_{1,3}$; $P^1_{2,2}$, $P^1_{2,3}$; …; $P^1_{m,2}$, $P^1_{m,3}$. Далее, из одной позиции $P^1_{1,2}$, $P^1_{2,2}$, или $P^1_{m,2}$ две метки уходят, преобразуются в одну метку согласно числу входящих и исходящих из перехода дуг в позицию P^{n-1}_1 для начала отсчета второго интервала времени (на рисунке интервала n–1). Идет отсчёт времени n–1 интервала до нажатия последней кнопки пароля с символом, соответствующим позиции P^n. Далее, осуществляется процесс аналогичный подсчету времени первого интервала, рассмотренного выше.

Позиция P^n_1 является завершающей и свидетельствует об окончании задания пароля.

Ввод пароля при аутентификации обладает следующими особенностями. Задается первый символ пароля меткой в позиции P^1_1. Начинается перемещение метки с учетом задержек в переходах. При правильном выборе пользователем паузы между первым и вторым символами пароля, метка окажется во второй позиции пар $P^1_{1,2}$, $P^1_{1,3}$; $P^1_{2,2}$, $P^1_{2,3}$; …; $P^1_{m,2}$, $P^1_{m,3}$, в первой из которых отсутствует метка. Вторая позиция

будет содержать три метки и из неё сформируется одна метка, которая поступит в позицию $P^{n-1}{}_1$ для продолжения распознавания пароля.

Необходимо отметить, что попадание меток в позиции $P^1{}_{m+1}$, $P^2{}_{m+1}\ldots$, $P^{n-1}{}_{m+1}$ свидетельствует об ошибке в наборе пароля. Появление метки в позиции $P^n{}_1$ свидетельствует о правильной аутентификации пользователя.

Сложность пароля

Для оценки эффективности противодействия описанного способа атакам методом подбора пароля, необходимо оценить сложность выполнения таких атак. Определим сложность как количество ресурсов, необходимых для успешного подбора пароля методом полного перебора. В качестве затрачиваемых ресурсов может выступать как количество машинных операций, так и связанное с ними время подбора. Любой из этих параметров напрямую зависит от числа перебираемых вариантов, которое можно определить по формуле:

$$V = b^c = \prod_{k=1}^{c} b, \qquad (2)$$

где V — общее количество вариантов, b — мощность алфавита, c — количество символов в пароле.

С учётом метода представления пароля, описанного формулой (1), формула (2) пример вид:

$$V = \prod_{k=1}^{c} b_S \times \prod_{k=1}^{c-1} b_T,$$

где b_S — мощность алфавита символов, вводимых пользователем, b_S — количество возможных отсчётов времени.

Как видно, добавление к паролю временны́х интервалов между вводом его символов увеличивает число вариантов перебора в b_T^{c-1} раз.

Будем исходить из того, что минимальная длина пароля ограничена административно до рекомендуемого значения в 8 символов, а временны́е

интервалы представляют собой дискретное значение в диапазоне [1, 5] секунд, тогда количество вариантов перебора увеличится в 5^7 = 78 125 раз.

Заключение

Как видно из приведённых выше вычислений, комплексирование пользовательского пароля путём его сочетания с временны́ми промежутками между вводом символов, позволяет значительно повысить сложность подбора такого пароля, или обеспечить равную сложность при меньшем количестве символов. При этом, необходимость выдерживать паузу перед вводом очередного символа практически исключает атаки на такую систему аутентификации методом полного перебора, за счёт значительного увеличения времени на каждую попытку подбора, и в целом повышает защищённость системы.

Литература

1. Жданова И.В., Быков Д.В. Варианты построения системы защиты электронных документов от копирования // Инженерный вестник Дона, 2012, №2 URL: ivdon.ru/ru/magazine/archive/n2y2012/825.

2. Панкратов С.А. Использование графической информации для защиты программного и информационного обеспечения // Инженерный вестник Дона, 2012, №2 URL: ivdon.ru/ru/magazine/archive/n2y2012/792.

3. Лапина Т.И., Лапин Д.В. Многофакторная аутентификация пользователей информационных ресурсов // Информационно-измерительные и управляющие системы. 2017. №5 (15). С. 37-42.

4. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. М.: Университетская книга, 2012. 598 с.

5. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. М.: ДМК Пресс, 2017. 434 с.

6. Чалая Л.Э. Метод идентификации пользователей информационных систем на основе многосвязного представления клавиатурного почерка // Системи обробки інформації. 2007. №9 (67). С. 98-101.

7. Васильев В.И., Ложников П.С., Сулавко А.Е., Еременко А.В. Технологии скрытой биометрической идентификации пользователей компьютерных систем // Вопросы защиты информации. 2015. №3(110). С. 37-47.

8. Aized, T., 2010. Advances in Petri Net: Theory and Applications. InTeOpP, 229 p.

9. Рытов М.Ю., Еременко В.Т., Горлов А.П. Автоматизация процесса оценки состояния защищенности объекта информатизации с использованием ингибиторных, вероятностных и раскрашенных сетей Петри от утечки информации // Информационная безопасность. 2015. №4 (18). С. 584-587.

10. Popova-Zeugmann, L., 2013. Time and Petri Nets. Springer, 209 p.

References

1. Zhdanova I.V., Bykov D.V. Inženernyj vestnik Dona (Rus), 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/825.

2. Pankratov S.A. Inženernyj vestnik Dona (Rus), 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/792.

3. Lapina T.I., Lapin D.V. Informatsionno-izmeritel'nye i upravlyayushchie sistemy. 2017. №5 (15). pp. 37-42.

4. Mel'nikov D.A. Organizatsiya i obespechenie bezopasnosti informatsionno-tekhnologicheskikh setey i system [Organization and security providing of information technology networks and systems]. M.: Universitetskaya kniga, 2012. 598 p.

5. Biryukov A.A. Informatsionnaya bezopasnost': zashchita i napadenie. [Information security: protection and attack]. 2-e izd., pererab. i dop. M.: DMK Press, 2017. 434 p.

6. Chalaya L.E. Sistemi obrobki informatsiї. 2007. №9 (67). pp. 98-101.

7. Vasil'ev V.I., Lozhnikov P.S., Sulavko A.E., Eremenko A.V. Tekhnologii Voprosy zashchity informatsii. 2015. №3 (110). pp. 37-47.

8. Aized, T., 2010. Advances in Petri Net: Theory and Applications. InTeOpP, 229 p.

9. Rytov M.Yu., Eremenko V.T., Gorlov A.P. Informatsionnaya bezopasnost'. 2015. №4 (18). pp. 584-587.

10. Popova-Zeugmann, L., 2013. Time and Petri Nets. Springer, 209 p.