ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А.С. Аксенов

МЕХАНИЗМ ВОССТАНОВЛЕНИЯ ДОСТУПА К АККАУНТУ ЦЕЛЕВОГО РЕСУРСА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОЧТЫ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Введение. С каждым днем количество взломанных электронных почтовых ящиков увеличивается. В интернете можно найти огромное количество программ для осуществления взлома. Аккаунт – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам[1]. Получив доступ к почте, злоумышленник также может получить доступ к различным аккаунтам интернет-ресурсов, которые были ассоциированы с данной электронной почтой. Это все происходит вследствие неудачной реализации системы восстановления пароля: если пароль от аккаунта забыт, его можно без особого труда восстановить путем отправки сообщения с инструкциями к ранее ассоциированной электронной почте. Следуя данной инструкции, злоумышленник также может получить доступ к аккаунту целевого ресурса. Эта схема является большой уязвимостью в информационной безопасности.

Данная работа описывает относительно простую схему восстановления, благодаря которой только лицо, являющееся непосредственным владельцем аккаунта, сможет восстановить доступ к нему. Эта схема заключается в следующем: на предварительном этапе – при регистрации аккаунта на целевом ресурсе – пользователь помимо пароля, вводит некоторый произвольный шаблон, на основе которого будет происходить процесс восстановления аккаунта в случае утраты пароля. Данный шаблон может включать следующие параметры:

- алфавит может включать буквы (А, Б, В, …), цифры (0,1,2, …);
- фиксированная длина (от 6 до 15 символов);
- определенный символ на *k*-ой позиции в шаблоне;
- знак «?» - отвечающий за пропуск 1 символа;
- знак «*» - отвечающий за пропуск *j* символов ($j = 0 \dots n$);

Алгоритм восстановления доступа к аккаунту целевого ресурса следующий:

1. Пользователь посылает запрос на восстановление.

2. Система отправляет на почту пользователя *n* различных комбинаций, лишь одна из которых удовлетворяет пользовательскому шаблону.
3. Пользователь ищет среди этих комбинаций ту, которая соответствует шаблону, и вводит ее в соответствующее место на целевом ресурсе.
4. В случае если пользователь неверно ввел комбинацию, он может осуществить повторный запрос. Количество повторов должно быть ограниченно настройками механизма восстановления. После неправильного ввода ключа определенного числа раз возможность восстановления аккаунта будет заблокирована на время, определенное настройками механизма восстановления.

Количество всевозможных комбинаций длины *n* символов для алфавита [А..Я, 0..9] составляет 43^n. Согласно принципу Кирхгофа[2], подразумевается, что злоумышленник знает механизм восстановления. Проведя дифференциальный криптоанализ, возможно определить лишь вероятность, с которой выбранное слово может являться ключевым. Для того, чтобы произвести статистическое сглаживание, необходимо обеспечить «достаточно» хороший генератор псевдослучайных чисел[3]. «Достаточность» заключается в том, чтобы статистически выровнять выходные последовательности как по длине, так по расположению в них элементов, исходя из выбранного шаблона, равносильно как и самой последовательности вхождения элементов в слово относительно ключевого[4].

Использование предложенной схемы можно проанализировать на следующем примере.

Пользователь при регистрации аккаунта целевого ресурса создает шаблон произвольного вида – например, «А?2*» , где ? - любой символ, * - любое количество символов. Общее количество символов передаваемых псевдослучайных комбинации содержится в пределах от 6 до 15.

В дальнейшем, в случае необходимости восстановления пароля система управления ресурсом присылает несколько вариантов комбинаций:

12Ф96А6Й 3Н435РФ83 8Ф789Ь9Я1 93Э64НЙ5ЖФ5 АО26КЗФ
Ф83К92АЦЫ1 0ГЕ383 8ЕО96Ф6П31Ш9 Ш04РЪЗДЗ 8ГЮФ536

Пользователь без труда сможет найти комбинацию, соответствующую его шаблону, в то время как злоумышленника данная схема заставит потрудиться.

В первую очередь злоумышленник может проанализировать первичное приближение – случай, когда шаблон может состоять только из двух элементов(0 – любая цифра, 1 – любая буква), получается следующее:

12Ф96А6Й	00100101
3Н435РФ83	010001100
8Ф789Ь9Я1	010000010
93Э64НЙ5ЖФ5	00100110110
АО26КЗФ	1000111
Ф83К92АЦЫ1	1001001110
0ГЕ383	011000
8ЕО96Ф6П31Ш9	011001010010
Ш04РЪЗДЗ	10011010
8ГЮФ536	0111000

Для каждой последовательности составляется разность по Хеммингу (табл. 1), на основе которой злоумышленник может выявить наиболее удаленные друг от друга последовательности, возможно претендующие на то, чтобы быть ключом. Цветом в таблице помечены значения, соответствующие максимальной разнице между последовательностями.

Табл. 1. – расстояния по Хеммингу между последовательностями

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1		4	3	2	4	5	2	1	7	3
2			3	3	3	6	2	3	5	4
3				6	5	5	1	2	6	2
4					3	6	1	6	5	4
5						3	5	5	2	7
6							4	7	2	4
7								1	5	1
8									8	2
9										5

В случаях с последовательностями 1 и 9, 5 и 10, 8 и 9 расстояние максимально. Таким образом, получается 5 комбинаций, претендующих на роль потенциального ключа (в том числе комбинация АО26КЗФ, которая соответствует шаблону пользователя). Но это лишь предположение, сделанное на основе первичного приближения. Возможность однозначно указывать конкретные буквы и цифры во много раз затрудняет дальнейший анализ, так как количество комбинаций, претендующих на роль потенциального ключа, приблизится к общему количеству высылаемых комбинаций.

Заключение

Данная схема позволяет идентифицировать непосредственного владельца аккаунта (естественно, лишь в случае сохранения в тайне выбранного шаблона для восстановления), а также не позволяет злоумышленнику, завладевшему чужой электронной почтой, получить доступ к ассоциированному аккаунту целевого ресурса. В случае полной блокировки злоумышленником электронной почты, возможно применение дополнительных организационных мер для восстановления доступа к ресурсу правомочного пользователя.

Литература

1. Учётная запись [Электронный ресурс]. – 2015. – Режим доступа: https://ru.wikipedia.org/wiki/Учётная_запись

2. Принцип Кирхгофа [Электронный ресурс]. – 2013. – Режим доступа: http://www.finam.ru/dictionary/wordf02470/?n=32

3. Брюс Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Текст] / М.: Издательство Триумф, 2002. 816 с.

4. Гмурман В.Е., Теория вероятностей и математическая статистика. Учеб. пособие для вузов. Изд.7-е,стер. / М.: Высш. шк.,1999. - 479 с.

Ю.В. Алейнов

О СПОСОБАХ РАЗМЕЩЕНИЯ ЛОЖНЫХ ЦЕЛЕЙ В СЕТИ ДЛЯ ОБНАРУЖЕНИЯ НАПРАВЛЕННЫХ АТАК

(Самарский государственный технический университет)

В настоящее время можно отметить возрастающую актуальность такого класса угроз, как направленные сетевые атаки (*APT*) [1]. Направленные атаки характеризуются особым типом поведения нарушителя, который старается как можно более незаметно, используя специально подобранные или самостоятельно разработанные инструменты и применяя их как можно точнее, внедриться в сеть конкретного объекта информатизации [2,3].

По мнению ряда исследователей, перспективным методом обнаружения такого типа атак является метод, основанный на внедрении ложных целей (*Honeypot*) в защищаемую сеть [4]. Ложные цели реализуются в виде специальных объектов, не участвующих ни в каких производственных процессах, протекающих в сети и не взаимодействующих в штатном режиме ни с какими другими системами. Среди достоинств данного метода можно отметить:

- возможность обнаружения атак неизвестного типа;
- низкую вероятность ложных срабатываний.

В то же время, использование данного метода осложнено относительно высокой сложностью реализации системы ложных целей (ЛЦ). Особенно следует отметить задачу размещения ловушек в сети. Очевидно, что от того, как размещены ЛЦ, зависит вероятность обнаружения нарушителя.

В рамках исследований на тему создания автоматизированных систем управления ложными целями ряд авторов затрагивал проблему размещения ловушек в сети, в связи с чем, на данный момент имеется несколько подходов к ее решению [4]. Однако анализ работ по этой тематике показывает, что сущест-