

Анализ подходов к выбору парольной системы защиты сервера ЛВС при подключении к нему пользователей сети

77-30569/380497

03, март 2012

Гасов В. М., Постников В. М.

УДК 004.056.5

МГТУ им. Н.Э. Баумана

chernen@bmstu.ru

Введение. Автоматизированные системы обработки информации, построенные на базе ЛВС, широко используются практически во всех областях человеческой деятельности. Одним из основных компонентов этих систем является сервер ЛВС, на котором хранится вся информация. К серверу ЛВС, кроме легальных пользователей, довольно часто обращаются и посторонние лица, которые стараются разными способами подобрать пароль для входа в сеть. К числу основных способов подбора пароля следует отнести следующие:

- подсмотр сотрудниками паролей, вводимых легальными пользователями сети;
- перебор посторонними лицами, в частности злоумышленниками, паролей в интерактивном режиме для нахождения требуемого пароля и подключения к серверу;
- перехват злоумышленниками паролей легальных пользователей, передаваемых по сети.

Поэтому к серверу ЛВС предъявляются особые требования по обеспечению информационной безопасности, которые включают

- конфиденциальность информации, т. е. защиту информации от несанкционированного доступа;
- целостность информации, означающую, что данные, которые находятся на сервере, обладают свойствами непротиворечивости, защищенности и актуальности;
- доступность информации, означающую, что легальный авторизованный пользователь сети имеет возможность в приемлемое время получить требуемую информацию, находящуюся на сервере сети.

Для обеспечения доступа к серверу ЛВС только авторизованных пользователей администратор сети использует систему защиты, которая обычно включает поддержку следующих основных функций:

1. Идентификация пользователя - процедура проверки регистрационного имени пользователя и сравнения его с данными, находящимися в системном файле, содержащем идентификаторы пользователей. В результате сравнения система делает вывод о наличии первого свойства легальности у пользователя, который подключается к серверу.

- 2 Аутентификация пользователя – процедура проверки подлинности пользователя по введенному им паролю. Если пароль пользователя введен верно, то делается вывод о наличии второго свойства легальности у пользователя, который подключается к серверу.
3. Адресация пользователя – процедура проверки разрешенного по времени входа в сеть и адреса компьютера (или компьютеров), с которых разрешен вход в сеть. Если условие выполнено, то делается вывод о наличии третьего свойства легальности у пользователя, который подключается к серверу. После этого данного пользователя относят к разряду легальных пользователей и ему разрешен вход в сеть.
- 4 Авторизация пользователя – процедура проверки полномочий и привилегий пользователя на предоставление ему возможности выполнять те действия, которые разрешил администратор сети. Средства авторизации контролируют доступ только легальных пользователей к ресурсам сети, предоставляя каждому пользователю набор только тех функций, которые ему разрешены.
- 5 Апелляция пользователя – процедура ведения и протоколирования действий, совершаемых пользователем на сервере ЛВС, которые влияют на безопасность информации, расположенной на этом сервере.

При этом первые три из перечисленных функций входят в состав парольной системы защиты сервера ЛВС.

Постановка задачи. Необходимо провести сравнительный анализ существующих подходов к выбору парольной системы защиты сервера ЛВС и дать рекомендации по количественному и качественному составу рабочих параметров парольной системы защиты.

Решение задачи. Детальный анализ целого ряда работ [1-10] показал, что парольную систему защиты сервера ЛВС (Y) можно представить в виде следующего набора параметров:

$$Y = (L, A, T, N, S, B, R)$$

Где L - длина пароля, т.е. количество символов в составе пароля.

A - мощность алфавита пароля, т.е. количество символов, которые могут входить в состав пароля

T - срок действия пароля, т. е. периодичность изменения пароля.

N - уникальность пароля, т.е. его повторяемость, определяет сколько раз новый пароль не должен повторять старый, или через сколько паролей новый пароль может повторить старый пароль.

S - количество входов в систему со старым просроченным паролем, после истечения срока его действия.

B - блокировка пароля после неверного его ввода, указывает сколько раз последовательно друг за другом пользователь может неверно набрать и ввести пароль.

R - режим разблокирования пароля, указывает через какой промежуток времени и какими средствами возможно провести разблокирование пароля для обеспечения подключения легального пользователя к сети.

Обычно при подключении к серверу пользователь сначала вводит имя регистрации, а затем пароль. Исходя из общих принципов безопасности, пароль при вводе не отображается на экране монитора. В случае несоответствия введенных имени

пользователя и/или пароля легальным значениям, а также при срабатывании блокировки регистрации, система отказывает пользователю в подключении к серверу и просит повторить подключение.

По истечении нескольких неудачных попыток подключения пользователя к серверу, число которых зависит от настройки системы администратором ЛВС и обычно составляет от трех до пяти попыток, система блокирует подключение пользователя к серверу. Время блокировки подключения пользователя к серверу обычно устанавливает администратор ЛВС и его можно изменять в широких пределах.

Для затруднения несанкционированным пользователям процесса подключения к серверу, администратор ЛВС в своей практической работе использует широкий набор параметров системы парольной защиты сервера, работающего под управлением сетевых ОС, что наглядно иллюстрируют данные, приведенные в табл.1

Таблица 1

Параметры парольной системы защиты сервера

№	Наименование параметров	Значение параметров сетевой ОС	
		Windows Server 2003	Netware 5
1	Количество символов в имени пользователя	от 1 до 20	от 1 до 32
2	Количество символов в пароле пользователя	от 1 до 14	от 1 до 128
3	Срок действия пароля в днях	от 1 до 999	от 1 до 365
4	Порог блокировки пароля, т. е. количество последовательных неудачных попыток подключения пользователя к серверу ЛВС, после которых подключение блокируется.	от 1 до 999	от 1 до 999
5	Интервал блокировки, т. е. время блокировки подключения пользователя к серверу до ее автоматической разблокировки	от 0 до 99999 мин	Дни от 1 до 365
			Часы от 1 до 23
			Мин от 1 до 59
6	Время подключения пользователя к серверу	В таблице «дни недели и часы (интервал 30 мин)», которая имеется в системе для каждого пользователя, администратор делает клетки пустыми для запрета этому пользователю входа в сеть во время, соответствующее этим пустым клеткам таблицы.	
7	Рабочие станции, с которых пользователю разрешено подключение к серверу	В учетной записи пользователя в соответствующей вкладке администратор указывает адреса рабочих станций, с которых этому пользователю разрешено подключение к серверу. Если поле пустое, то пользователю разрешено подключение к серверу с любых рабочих станций.	

Примечание.

- 1) Пароль должен содержать только разрешенные в ОС символы.
- 2) Если интервал блокировки равен нулю, то блокировка неверного ввода пароля отсутствует, и пользователь может осуществлять неверный ввод пароля бесконечное число раз, пока не наберет правильный пароль.

Вероятность (P) подбора злоумышленником пароля легального пользователя сети в течении срока действия этого пароля определяется из следующего выражения:

$$P = \frac{V \cdot T}{W} \quad (1)$$

Где T - срок действия пароля пользователя

V - скорость подбора пароля пользователя злоумышленником

W - мощность пространства паролей

$$\text{при этом } W = A^L \quad (2)$$

Где A - алфавит пароля

L - длина пароля пользователя при отсутствии режима блокировки ввода пароля

После подстановки выражения (2) в выражение (1) получаем

$$P = \frac{V \cdot T}{A^L} \quad (3)$$

После преобразования выражения (3) имеем:

$$A^L = \frac{V \cdot T}{P} \quad (4)$$

После дальнейшего преобразования выражения (3) из него получаем выражение для определения требуемой длины пароля пользователя в зависимости от заданного набора исходных данных: срока действия пароля пользователя, скорости подбора пароля пользователя злоумышленником, вероятности подбора пароля пользователя злоумышленником и мощности пространства паролей, которое имеет следующий вид

$$L = (\ln \frac{V \cdot T}{P}) / \ln A \quad (5)$$

Согласно [1-3] имеем следующие возможные значения для алфавита пароля $A = 10$ если для набора символов, входящих в состав пароля, используются только цифры от 0 до 9.

$A = 26$ если для набора символов, входящих в состав пароля, используются буквы латинского алфавита без изменения регистра

$A = 36$ если для набора символов, входящих в состав пароля, используются буквы латинского алфавита без изменения регистра и цифры от 0 до 9.

$A = 52$ если для набора символов, входящих в состав пароля, используются буквы латинского алфавита верхнего и нижнего регистров

$A = 62$ если для набора символов, входящих в состав пароля, используются буквы латинского алфавита верхнего и нижнего регистров, а также цифры от 0 до 9.

При этом, как правило, администраторы сетей в большинстве случаев используют следующие значения алфавита паролей $A = 36$ символов или $A = 62$ символа, которые учитывают как особенности клавиатуры компьютера, так и особенности работы пользователя за этой клавиатурой, а также требования сетевой ОС.

Сначала проведем выбор параметров парольной системы защиты сервера ЛВС без использования режима автоматической блокировки ввода пароля.

Согласно [1] наиболее часто администраторы сетей в своей практической работе в качестве срока действия пароля пользователя задают месяц, т. е.

$T=30$ суток = 720 час = $2,592 \cdot 10^6$ с, а скорость подбора пароля пользователя злоумышленником с использованием современных компьютеров, при отсутствии режима блокировки пароля, считают изменяемой в пределах от $V=10^5$ до $V=10^7$ символов/с.

Результаты расчетов, проведенных с использованием выражения (5) при подстановке в него следующих числовых значений исходных данных

- скорость подбора пароля пользователя злоумышленником $V=10^5$, $V=10^6$ и $V=10^7$ символов/с,
- вероятность подбора пароля пользователя злоумышленником от 10^{-3} с шагом 10^{-1} до величины 10^{-15} ,
- количество символов в алфавите пароля $A=36$ символов, $A=62$ символов, приведены в табл.2

Таблица 2

Рекомендуемое количество символов в пароле пользователя без использования режима блокировки ввода пароля

Вероятность подбора пароля Р	Длина пароля L (количество символов в составе пароля)					
	A=36			A=62		
	$V=10^5$	$V=10^6$	$V=10^7$	$V=10^5$	$V=10^6$	$V=10^7$
10^{-15}	16,98	17,63	18,28	14,72	15,29	15,84
10^{-14}	16,35	16,98	17,63	14,17	14,72	15,29
10^{-13}	15,70	16,35	16,98	13,61	14,17	14,72
10^{-12}	15,06	15,70	16,35	13,06	13,61	14,17
10^{-11}	14,43	15,06	15,70	12,50	13,06	13,61
10^{-10}	13,77	14,43	15,06	11,94	12,50	13,06
10^{-9}	13,13	13,77	14,43	11,38	11,94	12,50
10^{-8}	12,43	13,13	13,77	10,82	11,38	11,94
10^{-7}	11,84	12,43	13,13	10,28	10,82	11,38
10^{-6}	11,20	11,84	12,43	9,72	10,28	10,82
10^{-5}	10,56	11,20	11,84	9,15	9,72	10,28
10^{-4}	9,92	10,56	11,20	8,60	9,15	9,72
10^{-3}	9,28	9,92	10,56	8,04	8,60	9,15

Далее рассмотрим выбор параметров парольной системы защиты сервера ЛВС при использовании режима автоматической блокировки ввода пароля.

При использовании этого режима работы система, в случае нескольких (n) последовательных неверных попыток ввода пароля, будет автоматически осуществлять блокировку его дальнейшего ввода на некоторый промежуток времени, равный $T_{\text{бл}}$.

Скорость подбора пароля пользователя при наличии блокировки ($V_{\text{бл}}$) существенно снижается по сравнению с режимом отсутствия блокировки и определяется из следующего выражения

$$V_{\text{бл}} = \frac{n}{T_{\text{бл}}} \quad (6)$$

Типовые значения времени блокировки ввода пароля пользователя и скорости подбора пароля, вычисленные по выражению (6) при числе неверных попыток ввода пароля, равном трем ($n = 3$), которое наиболее широко используется администраторами сетей в их практической работе, приведены в табл. 3

Таблица 3

Скорость подбора пароля пользователя злоумышленником при наличии режима блокировки пароля при трех неверных попытках, $n=3$

Время блокировки ввода пароля, устанавливаемое администратором сети (мин)	$T_{\text{бл}}$ (с)	Скорость подбора пароля при наличии блокировки $V_{\text{бл}}$ (паролей/с)
60	3600	0,000833
30	1800	0,001666
15	900	0,003333
5	300	0,01
1	60	0,05

При использовании режима автоматической блокировки ввода пароля выражение для определения требуемой длины пароля пользователя в зависимости от заданного набора исходных данных: срока действия пароля пользователя, скорости подбора пароля пользователя злоумышленником, вероятности подбора пароля пользователя злоумышленником и мощности пространства паролей, с учетом выражений (5) и (6) имеет следующий вид:

$$L_{\text{бл}} = (Ln \frac{V_{\text{бл}} \cdot T}{P}) / LnA \quad (7)$$

Где $L_{\text{бл}}$ - длина пароля пользователя при наличии режима блокировки ввода пароля

Согласно выражению (7) получаем, что использование режима автоматической блокировки ввода пароля за счет резкого уменьшения скорости подбора пароля пользователя, по сравнению с режимом отсутствия такой блокировки, при прочих равных условиях (одинаковые значения параметров T, P, A), позволяет существенно уменьшить длину пароля, т. е. количество символов в пароле.

При этом количество символов (ΔL), на которое можно уменьшить длину пароля при наличии автоматической блокировки ввода пароля по сравнению с ее отсутствием, без изменения остальных параметров, можно определить из следующего выражения

$$\Delta L = L - L_{\text{бл}} = (Ln \frac{V \cdot T}{P}) / LnA - (Ln \frac{V_{\text{бл}} \cdot T}{P}) / LnA = (Ln \frac{V}{V_{\text{бл}}}) / LnA \quad (8)$$

При расчетах LnA принимает следующие значения $Ln36 = 3,58$ и $Ln62 = 4,13$

Исходные данные для расчета (A , V , $V_{\text{бл}}$) приведены в табл. 4. Значения ΔL , вычисленные по выражению (8) с учетом этих исходных данных, также приведены в табл. 4

Таблица 4

Уменьшение длины пароля пользователя за счет использования режима блокировки паролей по сравнению с ее отсутствием.

$V_{\text{бл}}$ (паролей/с)	Уменьшение длины пароля ΔL , т. е количества символов в составе пароля, за счет использования режима блокировки пароля					
	A=36			A=62		
	V=10 ⁵	V=10 ⁶	V=10 ⁷	V=10 ⁵	V=10 ⁶	V=10 ⁷
0,000833	5,20	5,84	6,48	4,50	5,06	5,62
0,001666	5,00	5,65	6,29	4,33	4,90	5,45
0,003333	4,80	5,45	6,10	4,16	4,73	5,28
0,01	4,50	5,15	5,79	3,92	4,46	5,02
0,05	4,05	4,70	5,34	3,51	4,07	4,63

Анализ результатов, приведенных в табл.4 показывает, что использование режима блокировки ввода пароля пользователя, по сравнению с ее отсутствием, позволяет уменьшить длину пароля пользователя в современных условиях развития компьютерной техники на 4 – 5 символов, обеспечивая надлежащий уровень защиты сервера ЛВС от проникновения на него злоумышленника..

Сокращение длины пароля пользователя важно по следующим двум факторам:

- легальный пользователь может выбрать требуемый по длине пароль, например, в десять и даже более символов, но достаточно простой по сложности, чтобы его легко было запомнить, но такой пароль и проще подобрать;
- легальный пользователь может выбрать требуемый по длине пароль, но сложный для запоминания, который записывает на бумаге и тем самым не обеспечивает конфиденциальность его хранения.

Результаты, полученные на основании проведенных исследований, а также результаты работ [1-3] позволяют дать следующие рекомендации администратору сети по формированию парольной системы защиты сервера ЛВС:

1. на сервере ЛВС целесообразно установить режим автоматической блокировки ввода пароля пользователя, при котором, после трех неверных попыток подключения

- пользователя к серверу, вход в сеть блокируется на некоторое время, например, от одной минуты до одного часа, однако достаточно и одной минуты;
2. пароль пользователя не должен содержать осмысленных слов из словаря, чтобы резко уменьшить скорость подбора пароля даже в случае использования компьютерной техники и тем самым усложнить злоумышленнику процесс подбора пароля пользователя;
 3. пароль пользователя должен соответствовать алфавиту $A=62$ и содержать разные группы символов, т. е. цифры, буквы, знаки препинания, включая символы верхнего и нижнего регистров;
 4. пароль пользователя соответствующий алфавиту $A=36$ не допускает переключение регистров, имеет меньшую мощность пространства паролей и поэтому требует практически на два символа больше для обеспечения той же вероятности подбора пароля, что и пароль, соответствующий алфавиту $A=62$;
 5. пароль пользователя должен содержать случайный набор не менее чем из 7 – 8 символов в алфавите $A=62$, чтобы обеспечить вероятность подбора пароля злоумышленником в пределах допустимой для практики величины от 10^{-5} до 10^{-8} . При этом, чем меньше алфавит пароля, тем длиннее пароль должен быть;
 6. пароль пользователя должен иметь ограниченный срок действия, но не более 30 суток;
 7. пароль пользователя должен быть составлен таким образом, чтобы достаточно просто и легко было запомнить метод его получения, а по возможности и сам пароль.

Выводы

1. На основе проведенного анализа работ по выбору парольной системы защиты сервера ЛВС выявлены функции, которые должна выполнять система защиты сервера и определен набор рабочих параметров, которые следует учитывать при формировании парольной системы защиты сервера ЛВС.
2. Показано, что использование режима блокировки ввода пароля позволяет резко сократить скорость подбора пароля и тем самым уменьшить длину пароля пользователя на 4 – 5 символов, обеспечивая надлежащий уровень защиты сервера ЛВС от проникновения на него злоумышленника в современных условиях развития компьютерной техники
3. Даны рекомендации по организации парольной системы защиты сервера ЛВС, направленные на обеспечение требуемого уровня информационной безопасности сервера ЛВС.

Литература

1. Абоенов А.Ж. Практическая методика оценивания параметров объектов защиты информации в информационной системе. / А.Ж. Абоенов, Г.А. Абоенова, Р.Н. Заркумова. – Новосибирск: Новосибирский гос. техн. ун-т., 2010. – 44 с.
2. Аникин И.В. / Теория информационной безопасности и методология защиты информации./ И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина. – Казань: Изд-во Казан. гос. техн. ун-та., 2008.- 280 с.
3. Борисов М.А. Основы аппаратно-программной защиты информации. / М.А. Борисов, И.В. Заведцев, И.В. Чижев.– М.: Книжный дом ЛИБРОКОМ, 2011.– 376 с.
4. Васильева И.Н. Информационные технологии и защита информации. / И.Н. Васильева, Е.В. Стельмашонок. – СПб.: СПбГИЭУ, 2011. – 272 с.

5. Гусева А.И. Работа в локальных сетях NetWare 3.12 - 4.1. – М.: Диалог – МИФИ, 1996. – 288 с.
6. Огороков В.А. Операционные системы: курс лекций. – Челябинск: Изд-во Челяб. гос ун-та., 2011. – 288 с.
7. Семенов Ю.К. Сетевая операционная система Netware / 386. – М.: Центр учебных и информационных технологий, 1994. – 352 с.
8. Тарзанов В.В. Информационные технологии в управлении качеством и защита информации. Часть 2./ В.В. Тарзанов, И.Н.Васильева, М.А. Шапченко.- СПб.: СПбГИЭУ, 2011. – 174 с.
9. Федоров В.В. Информационные технологии в логистике. – М.: Изд-во Российской таможенной академии, 2010. – 200 с.
10. Ячиков И.М. Методы и средства защиты компьютерной информации./ И.М.Ячиков, Ю.В. Кочержинская, М.М. Гладышева.– Магнитогорск, ПОУ ВПО МГТУ, 2011.– 172 с.

Analysis of approaches to password system selection for protection of LAN servers when connecting Net users

77-30569/380497

03, March 2012

Gasov V.M., Postnikov V.M.

Bauman Moscow State Technical University

chernen@bmstu.ru

This article covers the analysis of approaches to a password system formation for protection of a LAN server when connecting Net users. Basing on the demands of information security, main functions of the password system for server protection were identified. The authors determine a set of main components of the password system; it consists of the password length, password alphabet, password expiration date, password uniqueness and variants of password blocking modes. The authors present an analytical expression for evaluating the required password length which guarantees the given probability level of matching the password subject to the speed and time of matching, and also the password alphabet. In order to provide the required level of information security, the authors give practical recommendations on password system formation for protecting the LAN server when connecting Net users.

Publications with keywords: [password protection system](#), [length of password](#), [alphabet of password](#), [password's expiration date](#), [unicity of password](#), [password's blocking mode](#)
Publications with words: [password protection system](#), [length of password](#), [alphabet of password](#), [password's expiration date](#), [unicity of password](#), [password's blocking mode](#)

References

1. Aboenov A.Zh., Aboenova G.A., Zarkumova R.N. *Prakticheskaya metodika otsenivaniia parametrov ob"ektov zashchity informatsii v informatsionnoi sisteme* [Practical methods of estimating the parameters of the objects of information protection in the information system]. Novosibirsk, NSTU Publ., 2010. 44 p.
2. Anikin I.V., Glova V.I., Neiman L.I., Nigmatullina A.N. *Teoriia informatsionnoi bezopasnosti i metodologiya zashchity informatsii* [Theory of information security and methodology of information protection]. Kazan', KSTU Publ., 2008. 280 p.
3. Borisov M.A., Zavedtsev I.V., Chizhov I.V. *Osnovy apparatno-programmnoi zashchity informatsii* [Fundamentals of hardware and software data protection]. Moscow, Librokom Publ., 2011. 376 p.

4. Vasil'eva I.N., Stel'mashonok E.V. *Informatsionnye tekhnologii i zashchita informatsii* [Information technology and data protection]. St. Petersburg, SPbSUEE Publ., 2011, 272 p.
5. Guseva A.I. *Rabota v lokal'nykh setiakh NetWare3.12-4.1.* [Working in local networks NetWare3.12-4.1.]. Moscow, Dialog-MIFI Publ., 1996. 288 p.
6. Okorokov V.A. *Operatsionnye sistemy: kurs lektsii* [Operating systems: A course of lectures]. Cheliabinsk, ChSU Publ., 2011. 288 p.
7. Semenov Iu.K. *Setevaia operatsionnaia sistema Netware/386* [Network operating system Netware/386]. Moscow, Center for Education and Information Technologies, 1994. 352 p.
8. Tarzanov V.V., Vasil'eva I.N., Shapchenko M.A. *Informatsionnye tekhnologii v upravlenii kachestvom i zashchita informatsii. Ch. 2* [Information technology in quality management and data protection. Pt. 2]. St. Petersburg, SPbSUEE Publ., 2011, 174 p.
9. Fedorov V.V. *Informatsionnye tekhnologii v logistike* [Information technology in logistics]. Moscow, Rus. Customs Acad. Publ., 2010. 200 p.
10. Iachikov I.M., Kocherzhinskaia Iu.V., Gladysheva M.M. *Metody i sredstva zashchity komp'iuternoi informatsii* [Methods and means of computer information protection]. Magnitogorsk, MagSTU Publ., 2011. 172 p.