УДК 004.05

АНАЛИЗ ВРЕМЕННЫХ И СЛОЖНОСТНЫХ ХАРАКТЕРИСТИК ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ В ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА Unix

Д. В. Юркин,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет телекоммуникаций
А. В. Винель,
канд. техн. наук, ведущий научный сотрудник
ЗАО «НПФ ИНСЕТ», г. Москва
В. В. Таранин,
аспирант
Петербургский государственный университет путей сообщения

Описан подход к оценке вероятностно-временных характеристик протоколов аутентификации в операционных системах семейства Unix, основывающийся на теории вероятностных графов. Показано влияние действий нарушителя на работу протоколов аутентификации.

Ключевые слова *— криптографические протоколы, Unix OS, вероятностные графы.*

Введение

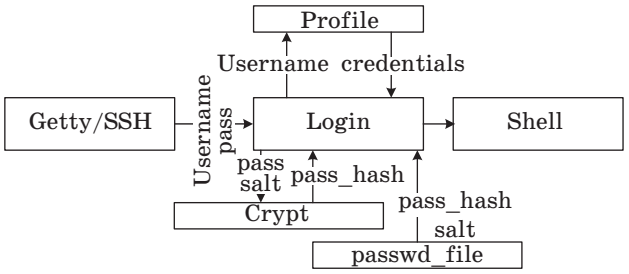
В мировой практике проектирования и построения защищенных информационных систем фактическим стандартом является использование Unix-подобных систем в качестве базовой операционной системы (ОС) для серверов и рабочих станций. Особый вклад в процесс эволюции защищенных ОС внесли ведущие разработчики и испытательные лаборатории систем обеспечения сетевой безопасности и средств защиты от несанкционированного доступа, которые на основании проводимых испытаний подтвердили отсутствие недекларированных возможностей, высокую отказоустойчивость встроенных механизмов защиты ОС. Портирование средств защиты информации Unix-подобных систем и широкий спектр поддерживаемых платформ привели к повсеместному использованию данных ОС производителями телекоммуникационного оборудования.

Правила реализации безопасной парольной политики и типовые настройки базовых встроенных механизмов управления доступом хорошо известны, однако вопрос анализа сложностных и временных характеристик успешного получения несанкционированного доступа к пользовательским и системным данным ОС на настоящий момент не подтверждены единым математическим доказательством.

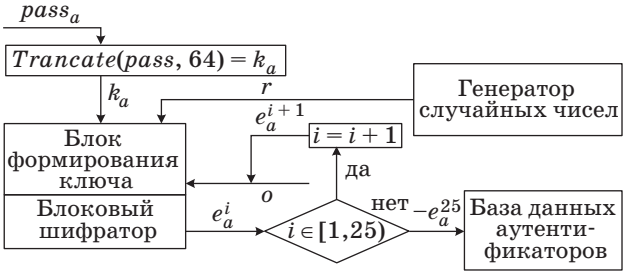
Описание способа парольной аутентификации

При предоставлении прав доступа к информационным ресурсам защищенной ОС возникает необходимость аутентификации пользователей для реализации механизмов дискретизации прав доступа. На данный момент наиболее распространенными и доступными ОС является семейство Unix, разработанное компанией Bell Laboratories. Встроенные механизмы зашиты таких ОС включают в свой состав протоколы парольной аутентификации [1], основой которых является верификация респондента по соответствию однонаправленного преобразования предъявленного пароля, приведенного в парольной таблице.

Взаимодействие программных модулей при аутентификации пользователей [2] осуществляется с вызова *getty* при непосредственном доступе с консоли и программных компонент пакета SSH при доступе с использованием сетевых средств управления программы *login*. Модуль *login* вызывается явно и замещает исходный интерпрета-



■ ***Рис. 1.*** Взаимодействие программных компонент при аутентификации субъектов в ОС



■ ***Рис. 2.*** Вычисление хеш-функции с использованием алгоритма DES

тор команд, после чего он выполняет проверку входных аутентификационных данных с использованием модуля криптографических преобразований *crypt* (или аналогичных). В случае успешной аутентификации *login* предоставляет доступ пользователю с соответствующими его профилю полномочиями к интерпретатору командной строки (рис. 1).

Вышеупомянутые криптографические преобразования могут быть реализованы выполнением функции шифрования с использованием ключа, полученного из пароля, конкатенированного с известной постоянной величиной и случайной последовательностью. В качестве однонаправленного преобразования может использоваться блоковое шифрование или ключевая хеш-функция. Ряд криптографических алгоритмов, реализуемых в схеме аутентификации (таблица), используются с добавлением к ключам случайных чисел.

В схеме однонаправленного преобразования по алгоритму DES (рис. 2) пароля $pass_a$ используется 25-кратное блоковое шифрование [3] нулевой последовательности o длиной 64 бита с добавлением битной случайной последовательности r с обратной связью, в качестве ключа k_a используются первые 64 бита пароля.

Добавление случайных чисел в алгоритм формирования ключей криптографического преобразования позволяет существенно затруднить атаку на базу аутентификаторов путем рандомизации его результатов. Поэтому алгоритмы перебора пароля при анализе базы данных увеличивают в общем случае трудоемкость вычислений в 2^r раза.

■ Используемые криптографические алгоритмы

Идентификатор алгоритма	Тип криптографического алгоритма
0	DES
1	MD5
2, $2a$, $2x$, $2y$	Blowfish
3	Алгоритм, совместимый с NT LAN Manager
4	SHA-1 (RFC 3174)
5	SHA-256 (RFC 4868)
6	SHA-512 (RFC 4868)

База аутентификаторов определяет соответствие идентификаторов пользователей, их символьных имен и соответствующих им хеш-функций паролей, а также другую информацию о пользователях и группах в системе. Этот массив данных представлен в виде текстовых файлов.

Существует два различных способа хранения паролей. Первый способ подразумевает общедоступное хранение аутентификаторов и хеш-функций паролей в едином файле вместе с реквизитами бюджетов пользователей. Второй, «теневой» способ ограничивает доступ пользователей к значениям хеш-функций паролей и определяет их размещение в отдельном файле, разрешенном на чтение и изменение только системным пользователям или процессам.

Очевидно, что «теневой» способ хранения значений однонаправленных криптографических функций паролей и случайных последовательностей позволяет увеличить защищенность системы аутентификации и повышает общий уровень робастности ОС относительно способов хранения аутентификационных данных, не использующих рандомизацию.

Однако при вышеописанном информационном обмене в процессе передачи данных инициатор провоцирует прямую компрометацию общего секрета. Это делает такую схему слабой аутентификации неприменимой в открытых каналах связи, а также предполагает ее использование только в доверенной среде передачи данных, что часто обеспечивается на практике посредством криптографической инкапсуляции передаваемых данных.

Методы формирования атак на протокол аутентификации

Рассмотрим применение методов теории вероятностных графов к моделированию различных схем взаимодействия участников информацион-

ного обмена в недоверенной среде передачи данных, состоящей из двух участников протокола (инициатора и респондента) и нарушителя. Предположим, что нарушитель имеет доступ к передаваемым сообщениям, поэтому может выполнять как перехват, так и подавление с подменой сообщения. Таким образом, взаимодействие корреспондентов информационного обмена происходит с участием посредника, который получает сообщения обоих легитимных сторон и может ретранслировать их без изменений, а может подменить любое сообщение на свое, и при этом факт подмены не будет замечен. Ориентированным графом покажем состояние схемы взаимодействия нарушителя и атакуемого легитимного корреспондента для протокола аутентификации (рис. 3).

Производящая функция перехода из состояния запроса аутентификации в состояние ее успешного завершения $f_r = 2^{-n}x_v^t$, а производящая функция перехода в начальное состояние протокола в случае предоставления неверных учетных данных равна $f_r^{err} = (1 - 2^{-n})x_v^t$. Общая производящая функция всего графа [4]

$$F(n) = \frac{f_r(n)}{1 - f_r^{err}(n)}.$$

Злоумышленник, получив запрос инициатора, пытается либо предугадать соответствующий ему ответ путем перебора общего секрета легитимных участников, либо просто угадать ответ. Предположим, что однонаправленное преобразование $R = f(S_{ab}, R)$ участники протокола выполняют идеально стойкой криптосистемой. Тогда вероятность того, что произвольно выбранное нарушителем значение S'_{ab} соответствует распределенному секрет, равна $P(S'_{ab} = S_{ab}) = 2^{-l(S_{ab})}$.

В случае, когда атакующий действует методом угадывания ожидаемого ответа, можно предположить, что все варианты отображения элементов множества запросов равновероятны. Тогда вероятность угадать ответ на i-й итерации $P(R'_i = R_i) = 2^{-l(R)}$. Таким образом, вероятность перехода из состояния r в состояние v будет $P(r \to v) = 2^{-n}$, где n — битовая длина перебираемой последовательности. Время, затрачиваемое верификатором на обработку одного запроса аутентификации, определяется величиной t_v. Согласно теории вероятностных графов [5], зависимость среднего времени успешного выполнения атаки угадыванием ответа от его длины с попыткой установления одной сессии протокола

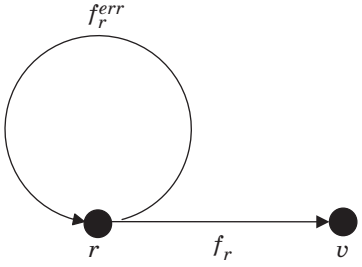
$$T_{e\_g}(n) = \frac{2^{-n} \cdot t_v \cdot (1 - (1 - 2^{-n})) + (1 - 2^{-n}) \cdot t_v \cdot 2^{-n}}{(1 - (1 - 2^{-n}))^2} = 2^n \cdot t_v.$$

Если атакующий действует методом перебора секретной последовательности, то очевидно, что с увеличением числа выполненных итераций протокола количество последовательностей, одна из которых является общим секретом легитимных корреспондентов, сокращается. Поэтому вероятность успешного перебора на i-й итерации $P(R'_i = R_i) = 2^{-(l(S_{ab})-i)}$. Таким образом, вероятность перехода из состояния r в состояние v равна $P(r \to v) = (2_s^n - i)^{-1}$, где n_s — битовая длина общего секрета. Зависимость среднего времени успешного выполнения атаки перебором секрета от его длины при попытке установления i сессий протокола

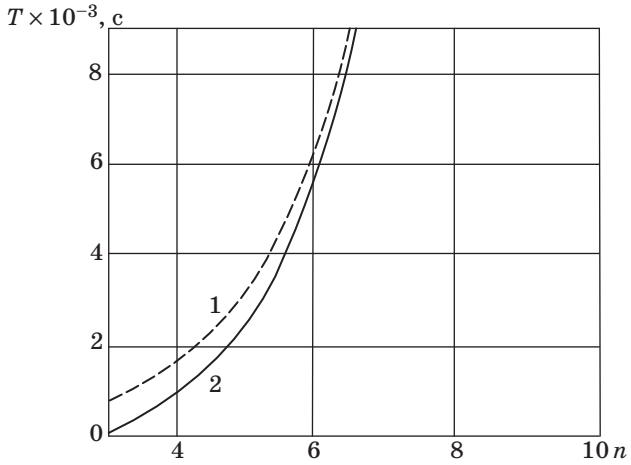
$$T_{e\_s}(n) = \frac{\frac{1}{2^n - i} \cdot t_v \cdot \left(1 - \left(1 - \frac{1}{2^n - i}\right)\right) + \left(1 - \frac{1}{2^n - i}\right) \cdot t_v \cdot \frac{1}{2^n - i}}{\left(1 - \left(1 - \frac{1}{2^n - i}\right)\right)^2} = (2^n - i) \cdot t_v.$$

Сравнение средних времен успешного выполнения атаки на протокол аутентификации перебором и угадыванием общего секрета представлено на рис. 4.

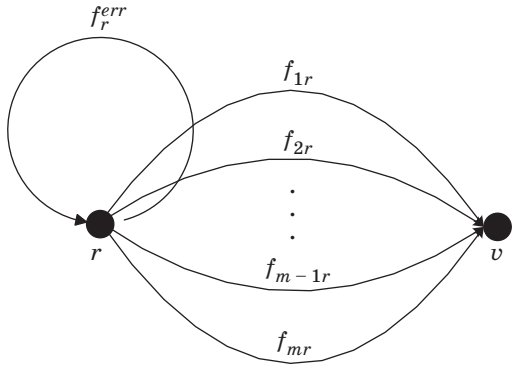
Однако наряду с последовательным выполнением итераций протокола атакующий также может одновременно начинать несколько сессий про-



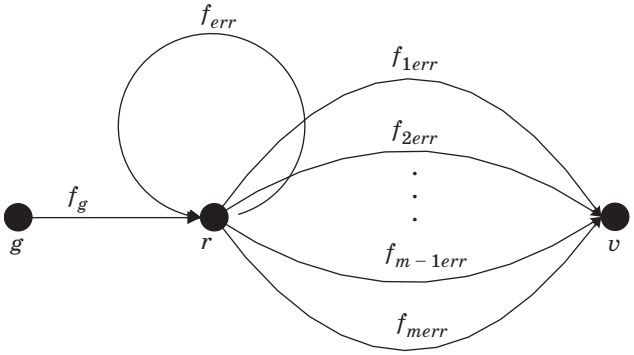
■ ***Рис. 3.*** Вероятностный граф протокола аутентификации



■ ***Рис. 4.*** Сравнение среднего времени атаки угадыванием (*1*) и перебором (*2*) общего секрета



■ ***Рис. 5.*** Вероятностный граф выполнения протокола аутентификации с инициализацией m параллельных сессий



■ ***Рис. 7.*** Вероятностный граф выполнения протокола аутентификации с инициализацией m параллельных сессий с предварительными вычислениями

токола, в этом случае вероятностный граф протокола будет иметь вид, показанный на рис. 5.

При этом общая производящая функция всего графа

$$F(n) = \frac{f_r(n)}{m(1 - f_r^{err}(n))},\ m \in \{1, \ldots, n\}.$$

Среднее время выполнения данного протокола для случая угадывания последовательности за одну (две, три и четыре) сессии $T_{e\_g}(n) = (2^n) \cdot t_v \cdot m^{-1}$ (рис. 6).

Если атакующий действует перебором общего секрета S_{ab} длиной $l(S_{ab}) = n$ с одновременным выполнением m сессий протокола, тогда ему на каждой попытке необходимо выполнить однонаправленное преобразование за время t_g, что, безусловно, увеличит время выполнения итерации протокола, которое станет равным $T_{e\_s}(n) = (2^n - m)(t_v + t_g) \cdot m^{-1}$. Создание дополнительной узловой точки формирования «словаря» возможных значений общего секрета перед вероятностным переходом означает вынесение детерминированной конструкции из циклической группы. Следовательно, не изменяя временной сложности итерации, можно понизить вычислительную сложность вероятностного цикла алгоритма. Вид вероятностного графа протокола показан на рис. 7.

В данном случае величина среднего времени

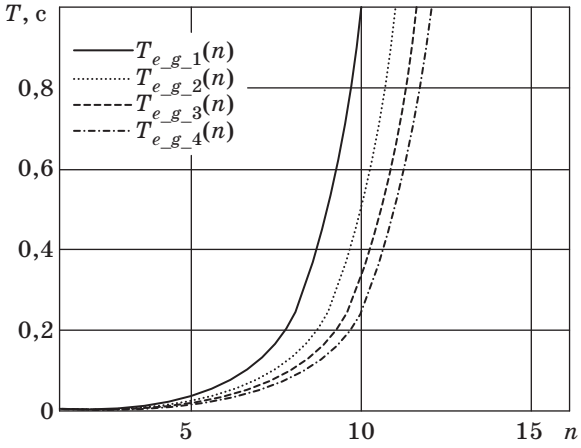
$$T_{e\_s}(n) =$$

$$= \frac{\frac{1}{2^n - m} \cdot (t_v + t_g)\left(1 - \left(1 - \frac{1}{2^n - m}\right)\right) + \left(1 - \frac{1}{2^n - m}\right) \cdot t_v \cdot \frac{1}{2^n - m}}{m\left(1 - \left(1 - \frac{1}{2^n - m}\right)\right)^2} =$$

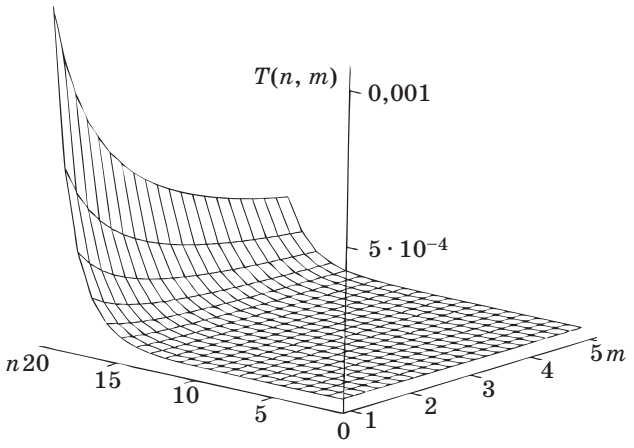
$$= m^{-1}((2^n - m) \cdot t_v + t_g).$$

Зависимость среднего времени выполнения протокола атаки от числа параллельных сессий и длины секрета в общем виде представлена на рис. 8.

Сравним результаты вероятностно-временного моделирования и теоретико-сложностных методов. Для этого произведем асимптотическую оценку функции трудоемкости алгоритма, определяющую сложность алгоритма и позволяю-



■ ***Рис. 6.*** Среднее время выполнения атаки на протокол угадыванием ответа



■ ***Рис. 8.*** Зависимость среднего времени выполнения атаки от числа сессий и длины секрета

щую выбрать предпочтения в использовании того или иного алгоритма для больших значений размерности исходных данных. Воспользуемся мажоритарной $O(g(n))$ оценкой, позволяющей дать верхнюю оценку для трудоемкости алгоритмов атак на протокол.

В случае атаки перебором ответа решаемая задача имеет экспоненциальную сложность, следовательно, асимптотическая оценка имеет вид $O(2^n)$.

Среднее время выполнения итерации протокола по алгоритму атаки, направленной на перебор ответа: $T(n) = \sum_{i=1}^{n} T(x) \cdot p(x)$, где $p(x)$ — вероятность появления входной последовательности x, а суммирование ведется по всем возможным входным последовательностям длины n. С учетом предположения о том, что при осуществлении однонаправленного криптографического преобразования все выходные последовательности равновероятны, $T(n) = T(x)$. Сопоставив значение среднего времени успешного выполнения протокола и асимптотическую ограничивающую сверху функцию $g(n)$, получим, что $T(n) = T(x)g(n)$, т. е. наиболее «близкой» (а в общем случае — равной) мажорирующей функцией будет сама трудоемкость алгоритма атаки с единичным постоянным множителем.

Таким образом, можно сделать вывод, что вероятностно-временной анализ посредством детального рассмотрения информационного взаимодействия корреспондентов позволяет находить методы линейного уменьшения среднего времени выполнения атаки перебором ответа, например запуском нескольких параллельных сессий.

Заключение

Результаты вероятностно-временного анализа алгоритмов атак на протокол парольной аутентификации в Unix-подобных системах соответствуют теоретико-сложностным оценкам трудоемкости выполнения этих атак, наглядно иллюстрируя возможные типы поведения нарушителя, дающие при этом четкое обоснование эффективности воздействия. Вероятностно-временные методы могут иметь широкое распространение при формировании свидетельства разработчика по стойкости функции безопасности объекта оценки AVA_SOF для проведения сертификационных испытаний средств защиты информации.

Литература

1. **Scott Mann, Ellen L. Mitchell, Mitchell Krell.** Linux system security. — Prentice Hall, 2003. — 617 p.
2. **Robert Morris, Ken Thompson.** Password Security: A Case History // Communications of the ACM. 1997. Vol. 22. P. 594–597.
3. **Philip Leong, Chris Tham.** Unix Password Encryption Considered Inside // USENIX. 1991. Vol. 3. P. 269–279.
4. **Nikitin V., Yurkin D., Chilamkurti N.** The influence of the cryptographic protocols on the quality of the radio transmission // Proc. of Intern. Conf. on Ultra Modern Telecommunications (ICUMT-2009), St.-Petersburg, Russia, Nov. 2009. P. 1–5.
5. **Никитин В. Н., Юркин Д. В.** Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.