IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015). – Warsaw (Poland), 2015. – P. 293–297.
4. Ding, Ian-Jiun Compression for the Feature Points with Binary Descriptors / Ian-Jiun Ding, Szu-Wei Fu, Ching-Wen Hsiao, Pin-Xuan Lee, Yen-Chun Chen // Proceedings of the 19th International Conference on Digital Image Processing. – 2014. – Taiwan. – P. 651–656.
5. Daguang, Jiang. Comparion and Study of Classic Feature Point Detection Algorithm / Jiang Daguang, Yiy Junkai // Proceedings of the 2012 International Conference on Computer Science and Service System. – 2012. – P. 2307–2309.
6. Schimid, C. Evaluation of Interest Point Detectors / C. Schimid, R. Mohr, C. Bauckhane // International Journal of Computer Vision, 2nd ed. – Vol. 37. – 2000. – P.151–172.
7. Прэт, У. Цифровая обработка изображений: в 2-х книгах / Прэт У.; пер. с англ. Д.С. Лебедев. – М.: Мир, 1982. – Кн. 2 – 480 с., ил.
8. Демьянович Ю.К. Введение в теорию вэйвлетов. Курс лекций / Ю.К. Демьянович, В.А. Ходаковский - Санкт-Петербург, 2007р. – 49 с.
9. База изображений: AT&T Laboratories Cambridge. – Режим доступа: http://www.cl.cam.ac.uk/research/dtg/attarchive/facesatglance.html.

Материал поступил в редакцию 08.01.16

ZAHORODNIA D.I. Method of Face Identification Based on Contour Characteristic Points

This paper proposes a method for characteristic points detection based on the wavelet analysis of the curvature function, which allowed the detail regulation of the characteristic point's allocation. It is proposed to implement person's identification using the identification vector, which is based only on the contour characteristic points. The proposed method of person's identification allows increasing of video surveillance system performance by reducing the size of information to be processed.

УДК 003.26:51:004(075.8)

Виссия Х.Е.Р.М., Галибус Т.В., Гафуров С.В., Каганович Д.М.

ЗАЩИТА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА ОСНОВЕ РАЗДЕЛЕНИЯ СЕКРЕТА

В настоящее время использование мобильных технологий стало практически универсальным и наиболее удобным способом своевременного доступа к информации и управления ею. Все чаще важные конфиденциальные данные хранятся и обрабатываются на мобильных устройствах, что требует наличия соответствующих защитных механизмов, специализированных под нужды обеспечения безопасности мобильных платформ. Наиболее высоким уровнем защиты должны обладать при этом мобильные устройства, которые используются в корпоративном секторе, поскольку данные, хранящиеся на таких устройствах, являются наиболее уязвимыми.

В данной работе рассмотрена разработанная авторами система аутентификации для мобильной платформы Android, в основе которой лежит полиномиальная модулярная СРС[1], описанная в стандарте СТБ 34.101.60 [10] и работе [2]. В сравнении со стандартной системой аутентификации, при использовании предложенного метода нет необходимости в хранении кода аутентификации (паттерн/PIN/пароль) на устройстве пользователя [5]. Кроме того, стандартная система безопасности Android подвержена ряду известных уязвимостей, например, CVE-2015-3860 [4], которая позволяет злоумышленнику получить доступ к устройству пользователя, минуя этап аутентификации. Предложенный нами метод аутентификации не использует данных стандартных системных сервисов, за счет чего является более устойчивым к подобного рода атакам.

Таким образом, в рамках предложенного метода гарантируется, что доступ к ключу имеется только у аутентифицированного пользователя. Это достигается за счет хранения ключа в разделенном виде (в качестве участников разделения секрета выступают устройство и пользователь). Предложенная система защиты пользовательских ключей в мобильных приложениях является первой системой на основе разделения секрета, обладает хорошей встраиваемостью и может быть легко адаптирована для использования с существующими протоколами безопасности (SSL/TLS и т.п.).

Математические алгоритмы в основе аутентификации

1. (2, 2)-пороговая модулярная СРС

Рассмотрим (2, 2)-пороговую СРС [10], [2]. Алгоритм разделения секрета в этом случае принимает следующий вид:

1. Сгенерировать случайные попарно различные неприводимые многочлены $p_0(x), p_1(x), p_2(x); p_i(x) \in F_2[x], \deg p_i(x) = l+1, i = \overline{0,2}$;
2. Сгенерировать случайный равномерно распределенный одноразовый ключ $k(x) \in F_2[x], \deg k(x) = l$ и вычислить промежуточный секрет $S(x) = s(x) + kp_0(x)$;
3. Дилер публикует $p_i(x), i = \overline{0,2}$;
4. Дилер вычисляет частичные секреты $s_i(x) = S(x) \bmod p_i(x), i = \overline{1,2}$ и передает их участникам.

Алгоритм восстановления секрета имеет вид:

1. Участники передают вычисляющему устройству (дилеру) секреты $s_i(x), i = \overline{1,2}$;
2. Дилер вычисляет промежуточный секрет $S(x)$:

$$S(x) \equiv s_1(x)p_2(x)p_2^{-1}(x)_{p_1(x)} + \\ + s_2(x)p_1(x)p_1^{-1}(x)_{p_2(x)} \bmod p_1(x)p_2(x),$$

где $p_i^{-1}(x)_{p_j(x)} := p_i^{-1}(x) \bmod p_j(x)$.

3. Участники восстанавливают секрет $s(x) = S(x) \bmod p_0(x)$.

2. Генерация приватного ECDSA ключа

Стандарт ANSI X9.62[1] генерации приватного ECDSA не учитывает опасность использования ключей с малым весом Хемминга в NAF-

Виссия Херман Элизабет Мария Рене, *начальник филиала ИУП "Байлекс Малтимедиа", e-mail: h.vissia@byelex.com.*
Гафуров Сергей Владимирович, *начальник отдела филиала ИУП "Байлекс Малтимедиа".*
Каганович Дмитрий Михайлович, *студент кафедры информационных систем управления Белорусского государственного университета, сотрудник филиала ИУП "Байлекс Малтимедиа".*
Беларусь, 220028, г. Минск, ул. Маяковского, 111.
Галибус Татьяна Васильевна, *доцент кафедры информационных систем управления Белорусского государственного университета.*
Беларусь, 220013, г. Минск, пр. Независимости, 4.

[1] Схема разделения секрета

представлении [7], [8]. Поэтому для реализации системы защиты мы предлагаем следующую модификацию алгоритма генерации ключа.

Пусть (E,G,n) – эллиптическая кривая в поле F_{2^m}, где E – все множество точек кривой вместе с точкой в бесконечности o; G – базовая точка кривой ($G \neq o$); n – порядок базовой точки. Согласно [3], вес Хемминга $H(\bullet)$ NAF-представления случайного бинарного слова w, полученного из равномерного распределения, имеет нормальное распределение с математическим ожиданием $E(H(w_{NAF})) = \frac{\|w\|}{3} + \frac{4}{9} + O(2^{-\|w\|})$ и дисперсией $Var(H(w_{NAF})) = \frac{2\|w\|}{27} + \frac{14}{81} + O(\|w\|2^{-\|w\|})$, где $\|\bullet\|$ – битовая длина слова. Согласно [1], приватный ключ d выбирается из отрезка $[1, n-1]$. Если при этом требуется, чтобы $H(d_{NAF}) > \frac{\|n\|}{4}$, то доля отброшенных ключей составит $CDF_{N(E,\sigma)}(\frac{\|n\|}{4})$. Делитель 4 выбран, исходя из вида формул математического ожидания и дисперсии распределения весов, и гарантирует оптимальное время работы алгоритма генерации безопасного ключа.

Таким образом, модифицированный алгоритм генерации приватного ECDSA ключа включает генерацию ключа d в соответствии с ANSI X9.62 [1] и проверку условия $H(d_{NAF}) > \frac{\|n\|}{4}$. Генерация считается завершенной, если удалось найти такое d, что указанное неравенство выполнилось.

Протокол разделенного хранения секрета. Реализованная авторами система аутентификации основана на разделенном хранении пользовательского ключа. При этом ключи ECDSA генерируются устройством. Также, устройство выступает в роли дилера при разделении приватного ключа. Использование СРС позволяет гарантировать, что доступ к ключу может быть получен только аутентифицированным пользователем. Участниками (2, 2)-пороговой СРС являются устройство и пользователь. Частичный секрет пользователя $s_1(x)$ вычисляется на основе PIN-кода, который вводится пользователем на этапе инициализации ключей. Пусть $s(x) := d$ и $s_1(x) := f(PIN)$, где f – необратимая функция, преобразующая аргумент в октетную строку необходимой длины:

$$\begin{cases} S \equiv s \bmod p_0; \\ S \equiv s_1 \bmod p_1 \end{cases}$$

По китайской теореме об остатках решение системы может быть вычислено следующим образом:

$$S \equiv s_1 p_0 p_0^{-1}{}_{p_1} + s p_1 p_1^{-1}{}_{p_0} \bmod p_0 p_1 .$$

Вычисленный таким образом частичный секрет устройства записывается в постоянную память. Частичный секрет пользователя не записывается. В противном случае это бы позволило злоумышленнику локально проверять корректность восстановленного приватного ключа. Ключ сохраняется только на сервере с соблюдением мер конфиденциальности и целостности данных.

Несмотря на то, что открытый ключ не хранится на устройстве пользователя, для злоумышленника по-прежнему существуют три возможности проверить недействительность восстановленного ключа без отправки запроса на сервер:

1. Злоумышленник может быть в состоянии вычислить вес Хемминга NAF-представления восстановленного приватного ключа d' и проверить условие $H(d'_{NAF}) > \frac{\|n\|}{4}$ на выполнимость. Но при выборе делителя равного 4, процент недействительных по этому критерию ключей будет мал.
2. Злоумышленник может проверить, принадлежит ли восстановленное число промежутку $[1, n-1]$. Существует два способа решения этой проблемы: использование эллиптической кривой с максимально высоким порядком генератора или использование дополнительной октетной строки $q, \|q\| \geq \|n\|$. Для того, чтобы метод, основанный на использовании дополнительной строки, был применим на практике, последний должен гарантировать равномерность рапределения приватного ключа d.
3. Поскольку в рассматриваемой СРС длины открытых ключей совпадают с длиной исходного секрета, то для злоумышленника не составит труда установить действительную степень восстанавливаемого полинома. Учитывая идеальность СРС, это позволит ему при восстановлении в 50% случаев верно указать на недействительный ключ. Поэтому в системе обязательно должен присутствовать счетчик неудачных попыток аутентификации пользователя с наперед заданным пороговым значением, по превышении которого ключ пользователя будет считаться скомпрометированным.

Защищенный протокол авторизации и запроса документа. Рассмотрим интеграцию разработанной системы аутентификации с протоколом запроса защищенного документа клиентским устройством у сервера.

Инициализация ключей:

1. При первом обращении клиенту на почту отправляется одноразовый авторизационный код. Клиент узнает авторизационный код, затем генерирует секрет s. На основе полученного секрета клиент генерирует пару ключей (d,Q).
2. Клиент отправляет открытый ключ на сервер при помощи сообщения, которое содержит авторизационный код и открытый ECDSA ключ. Если авторизационный код совпадает с кодом на сервере, то ключ сохраняется на сервере. В случае некоторого числа неудачных попыток (как правило, трех), авторизационный код блокируется сервером и клиенту на почту отправляется новое письмо.
3. Клиент задает свой четырехзначный PIN-код. Секрет s разделяется при помощи PIN-кода, затем частичный секрет s_2 вместе с открытыми ключами записывается на устройство пользователя. Открытый ключ ECDSA не сохраняется на устройстве.

Последующие обращения клиента:

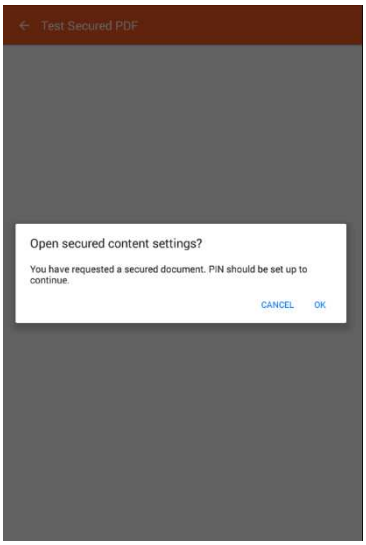
1. Пользователю предлагается ввести его PIN-код. С помощью PIN-кода клиента восстанавливается секрет s. На основе полученного значения клиентское устройство восстанавливает приватный ключ пользователя и подписывает им запрос на получение документа при помощи ECDSA.
2. Сервер верифицирует запрос. В случае предопределенного числа неудачных попыток, ключ пользователя считается скомпрометированным и пользователю предлагается пройти процесс инициализации ключей. Если запрос верифицирован, то сервер генерирует одноразовые симметричный ключ K и вектор инициализации $nonce$, с помощью которых шифрует документ, используя AES128/GCM. Затем, K и $nonce$ шифруются открытым ключом клиента (используется гибридная схема ECIES). K, $nonce$ и зашифрованный документ отправляются обратно клиенту.
3. Клиент с помощью своего приватного ключа расшифровывает K и $nonce$. Далее, клиент использует их для расшифрования полученного защищенного документа.

Апробация и тестирование

Описанная в предыдущем пункте схема использования разработанной системы аутентификации в протоколе запроса защищенного документа была реализована в приложении BuzzTalk Reader(Byelex Multimedia Products B.V.) (доступно для скачивания на Google Play).

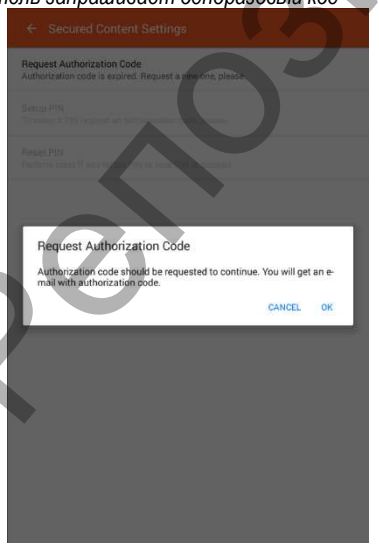
Ниже отображен процесс конфигурации пользователем настроек безопасности приложения (первые три шага пункта 3):

1. *Пользователь впервые пытается открыть защищенный документ*

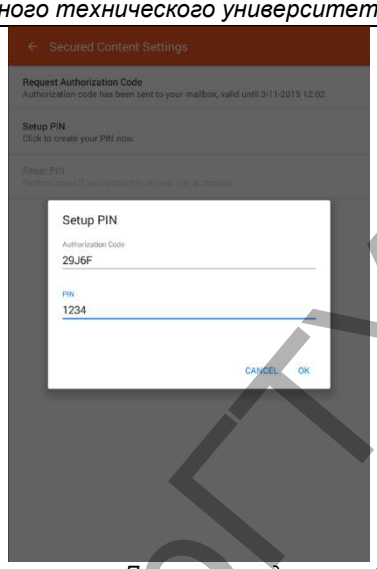


2. *Экран настроек безопасности по умолчанию*

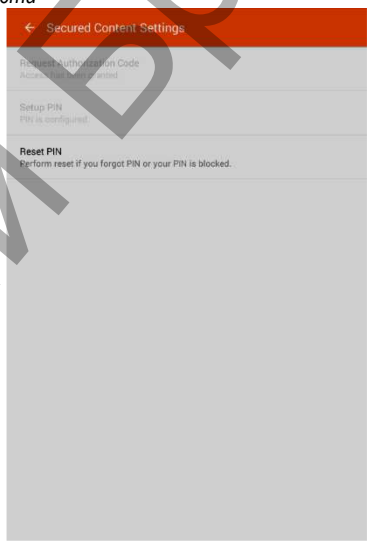
3. *Пользователь запрашивает одноразовый код*



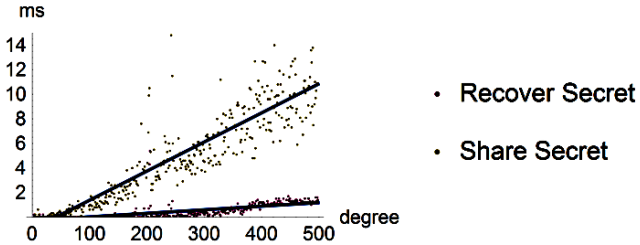
4. *Пользователь задает PIN код. Генерируется пара ключей. Разделяется приватный ключ. Открытый ключ отправляется на сервер*



5. *Настройка завершена. Пользователю доступен сброс настроек безопасности*



Одним из основных функциональных блоков рассматриваемой системы аутентификации является схема разделения приватного ключа. Поэтому в процессе разработки системы был проведен ряд испытаний, целью которых было установить зависимость времени работы алгоритмов разделения и восстановления секрета от длины используемого ключа (т.е. от длины входных данных). Суть испытаний заключалась в многократной симуляции процессов разделения и восстановления для секретов со степенями вплоть до 500 и последующем усреднении результатов. На диаграмме ниже представлены результаты серии испытаний, которые проводились на устройстве Google Nexus 7 Android 5.1.0. Также на рисунке выделены линии регрессии для упрощения анализа полученной выборки значений:



Как следует из диаграммы, процесс разделения ключа занимает значительно больше времени процесса его восстановления, что обоснованно с точки зрения теории. Дополнительный анализ показал, что около 95% всего времени разделения занимает процедура генерации открытых ключей СРС. Недостаточной детерминирован-

ностью этой процедуры объясняется и значительно больший разброс значений выборки относительно регрессионной линии.

Заключение. В работе предложена система аутентификации в мобильном приложении на основе разделенного хранения ключа ECDSA при помощи (2, 2)-пороговой полиномиальной модулярной СРС. С целью повышения стойкости алгоритмы разделения секрета и генерации ключей были модифицированы, что позволило реализовать защиту мобильного приложения наиболее эффективным образом. Система интегрирована с безопасным протоколом передачи защищенных документов мобильного приложения BuzzTalk Reader. Продемонстрировано использование системы и проанализированы результаты тестирования системы.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. American National Standard X9.62-1999, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA) / Accredited Standards Committee X9. – 1999. – P. 16.
2. Asmuth, C.A. A modular approach to key safeguarding / C.A. Asmuth, J. Bloom // IEEE Transactions on Information Theory. – 1983. – Vol. 29. – P. 156–169.
3. Heuberger, C. Prodinger Hamming Weight of the Non-Adjacent-Form under Various Input Statistics / C. Heuberger, H. Prodinger // Periodica Mathematica Hungarica. – Volume 55. – Issue 1: сб. науч. ст. – 2007. – P. 81–96.
4. Common Vulnerabilities and Exposures. The Standard for Information Security Vulnerability Names – Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3860. – Дата доступа: 06.11.2015.
5. Elenkov, N. Android Security Internals: An In-Depth Guide to Android's Security Architecture / Nikolay Elenkov. – San Francisco: No Starch Press, 2014. – P. 268–277.
6. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // Proc. of SYNASC'08. – IEEE Comp. soc. press, Los Alamitos – 2009 – P. 197-200.
7. J. A. Muir D. R. Stinson On the low weight discrete logarithm problem for nonadjacent representations / J. A. Muir D. R. Stinson // Applicable Algebra in Engineering, Communication and Computing Volume 16 Issue 6: сб. науч. ст. – 2006. – P. 461–472.
8. Schirokauer, O. The number field sieve for integers of low weight / Oliver Schirokauer // Mathematics of computation. – Volume 79. – Number 269: сб. науч. ст. – 2009. – P. 583–602.
9. Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters / Certicom Research. – 2010. – P. 13–26.
10. Информационные технологии и безопасность. Алгоритмы разделения секрета: СТБ 34.101.60-2014 – Минск: БГУ, 2014. – Режим доступа: http://apmi.bsu.by/assets/files/std/bels-spec29.pdf. – Дата доступа: 06.11.2015.

VISSIYA H.E.M.R., GALIBUS T.V., GAFUROV S.V., KAGANOVICH D.M. Mobile device authentication system based on the secret sharing scheme

In this paper, we propose a novel approach to the mobile authentication systems based on the secret sharing scheme.

The proposed approach provides a secure way to store a private key on a mobile device. In order to improve the functionality of the authentication system, we suggest a modification of ECDSA private key generation algorithm. We discuss the specifics of implementation and its integration into a secure transport protocol. We demonstrate the workflow of the production ready mobile application using the proposed protocol. Finally, we provide the results of mobile application testing along with analysis.

УДК 004.75

Цаволык Т.Г., Яцкив В.В.

МЕТОД ИСПРАВЛЕНИЯ ОШИБОК НА ОСНОВЕ МОДУЛЯРНЫХ КОРРЕКТИРУЮЩИХ КОДОВ

Введение. С развитием и широким использованием беспроводных технологий задача обеспечения высокой надежности передачи данных приобретает все более важное значение. В настоящее время для повышения надежности передачи данных разработаны и используются различные помехоустойчивые коды [1]. При выборе помехоустойчивых кодов необходимо учитывать сложность алгоритмов кодирования / декодирования, аппаратные ограничения устройств с автономным питанием, а также использование нелицензионного диапазона частот, что повышает вероятность искажения информационных символов.

Для повышения надежности передачи данных в беспроводных сенсорных сетях предложены модулярные корректирующие коды [2]. Данные коды сохраняют преимущества корректирующих кодов системы остаточных классов, но в отличие от последних обрабатывают входные данные, представленные в позиционной системе счисления (двоичной, десятичной), что значительно упрощает процедуры кодирования / декодирования и расширяет область их применения. В [3] разработан метод и алгоритм исправления многократных ошибок на основе модулярных корректирующих кодов с использованием двух проверочных символов.

Модулярные корректирующие коды. В данной работе разработан метод исправления ошибок в двух информационных символах с использованием одного проверочного символа. Значение контрольного символа в модулярных корректирующих кодах вычисляется по формуле [3]

$$x_{k+1} = \left|(v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i + \ldots + v_k \cdot x_k)\right|_P, \quad (1)$$

где x_i – информационные символы, v_i – коэффициенты взаимно простые с P, $|\bullet|_P$ – операция получения остатка по модулю P.

Декодер по принятым данным $\left(x_1^{'}, x_2^{'}, \ldots, x_i^{'}, \ldots, x_k^{'}\right)$ вычисляет значение контрольного символа:

$$x_{k+1}^{'} = \left|(v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i^{'} + \ldots + v_k \cdot x_k)\right|_P. \quad (2)$$

Для определения ошибки вычислим синдром, представляющий разницу между проверочным символом полученным и проверочным символом вычисленным на приемной стороне (в декодере):

$$\delta = \left|x_{k+1}^{'} - x_{k+1}\right|_P, \quad (3)$$

уравнение (3) можно записать в виде

Цаволык Тарас Григорьевич, *аспирант Тернопольского национального экономического университета.*

Яцкив Василий Васильевич, *к.т.н., доцент кафедры специализированных компьютерных систем Тернопольского национального экономического университета.*

Украина, 46009, г. Тернополь, Тернопольская область, ул. Львовская, 11.