2. *Колегов Д. Н., Ткаченко Н. О., Чернов Д. В.* Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL //Прикладная дискретная математика. Приложение. 2013. № 6. С. 62–67.
3. *Hinz S., DuBois P., and Stephens J.* MySQL 5.7 Reference Manual. `http://dev.mysql.com/doc/refman/5.7/en/mysql-proxy.html`
4. *Ierusalimschy R., Henrique de Figueiredo L., and Celes W.* The Programming Language Lua. Lua 5.2 Reference Manual. `http://lua.org/manual/5.2/`

УДК 004.056.57

МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-МАГАЗИНОВ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Е. А. Толюпа

Предложен метод противодействия распространению вредоносного ПО через интернет-магазины Android-приложений. Метод основан на применении доверенных цифровых подписей (ДЦП) и алгоритма (n, t)-пороговой ДЦП с арбитром, который позволяет разработчику антивирусного ПО реализовать механизм распределения доверенности и права проверки приложений на наличие вредоносного кода между n центрами проверки таким образом, что ДЦП будет вычислена только с участием арбитра и только в том случае, если t $(t < n)$ центров проверки подтвердят отсутствие вирусов. Роль арбитра можно возложить на удостоверяющие центры. Таким образом, проверяющий доверяет разработчику антивирусного ПО и удостоверяющему центру (арбитру) и может не опасаться, что центр проверки окажется злоумышленником и подпишет небезопасное приложение. Предложенный метод могут использовать интернет-магазины для повышения уровня доверия к себе среди потенциальных клиентов.

Ключевые слова: *антивирусная защита, доверенные цифровые подписи, пороговые доверенные цифровые подписи, Android, магазин приложений Android.*

Бурное развитие платформы Android повлекло создание большого числа интернет-магазинов Android-приложений. На сегодняшний день популярностью пользуются Google Play, Яндекс.Store, Amazon mobile app distribution, Samsung Apps, SlideMe, GetJar. Пётр Меркулов, директор по развитию продуктов и услуг Лаборатории Касперского, утверждает: «Магазины приложений для Android — это лакомый кусочек для вирусописателей. ... 99 % всех обнаруженных в 2012 г. мобильных зловредов были нацелены на Android-устройства». В 2012 г. Google запустил сервис Bouncer, который представляет собой виртуальную машину, эмулирующую окружение Android и осуществляющую динамический анализ приложений. Магазин Яндекс.Store проверяет антивирусом своё приложение. Таким образом, пользователи вынуждены доверять процедуре проверки файла самого магазина. Пользователь может доверять крупным корпорациям, имеющим положительную репутацию.

Платформа Android является открытой, и любой может разрабатывать свои приложения и публиковать их в сети или создать свой магазин приложений. Пользователь вынужден доверять тому, кто публикует приложения в сети. Интернет-магазин может оказаться злоумышленником и публиковать приложения, утверждая, что они проверены антивирусом. Возможен вариант, когда интернет-магазин может отправить файл на проверку надёжному разработчику антивирусного ПО (АПО), чтобы тот, проверив файл, сформировал электронную подпись (ЭП). Наличие корректной ЭП для файла является гарантией отсутствия вредоносного ПО. В этом случае разработчик АПО

должен иметь широкую филиальную сеть по всему миру или единый мощный центр, в котором все файлы приложений будут проверяться на наличие вредоносного ПО. Таким образом, затрудняется продвижение небольших магазинов, и открытость платформы может не дать ожидаемого эффекта в её продвижении.

Выходом может служить передача процедуры проверки распределенным центрам. В работе автора [1] предложен метод антивирусной защиты конечных устройств, основанный на применении доверенных цифровых подписей [2] и алгоритма (n, t)-пороговой ДЦП с арбитром. Алгоритм (n, t)-пороговой ДЦП с арбитром позволяет *разработчику АПО* реализовать механизм распределения *доверенности* и права проверки приложений на наличие вредоносного кода между n *доверенными центрами проверки* таким образом, что ДЦП будет вычислена только с участием *арбитра* и только в том случае, если t центров проверки подтвердят отсутствие вирусов. Арбитру должны доверять все участники системы. В качестве арбитра может выступать удостоверяющий центр (элемент PKI).

Взаимодействие участников представлено на рис. 1.

Подготовительный этап:

1. Разработчик АПО передаёт программное обеспечение для проверки файлов на наличие вредоносного кода и делегирует право проверки n центрам проверки.
2. Разработчик АПО передаёт удостоверяющему центру, который является арбитром, информацию, необходимую для вычисления ДЦП. Раскрытие информации третьим лицам ведёт к компрометации всей системы.

Проверка приложения:

3. Интернет-магазин передаёт файл с приложением (Android Package, APK-файл) t центрам проверки.
4. Каждый центр проверки с использованием программного обеспечения разработчика проверяет файл на наличие вредоносного кода и в случае успешной проверки вычисляет свою *долю* ДЦП и передает её арбитру.
5. Арбитр завершает вычисление ДЦП и передаёт полученное значение в интернет-магазин.
6. Интернет-магазин публикует APK-файл вместе с ДЦП.
7. Пользователь получает из интернет-магазина APK-файл и ДЦП для него. Убедившись в корректности ДЦП, вычисленной t центрами проверки, принимает решение, что приложение не содержит вредоносного кода.

В приведённой схеме пользователь доверяет разработчику АПО и арбитру. Он может не опасаться, что центр проверки окажется злоумышленником, так как ДЦП может быть сформирована только в том случае, если t из n ($t < n$) центров проверки подтвердят безопасность файла, проверив его антивирусным программным обеспечением разработчика. Файл будет ненадёжным, если все t центров окажутся злоумышленниками. Таким образом, разработчику АПО нет необходимости создавать собственную филиальную сеть, а проверка файлов будет производиться на вычислительных ресурсах центров проверки, с которыми разработчик установит партнёрские отношения. Таким образом, строится модель с участниками инфраструктуры, которым доверяет пользователь. Предложенный метод антивирусной защиты могут использовать интернет-магазины для повышения уровня доверия к себе среди потенциальных клиентов.

В рамках данного исследования разработано приложение для платформы Android, которое вычисляет ДЦП для APK-файлов. Тестирование проводилось на мобильных телефонах с процессором Samsung Exynos 4412 (1,4 ГГц) и Samsung Exynos 4210

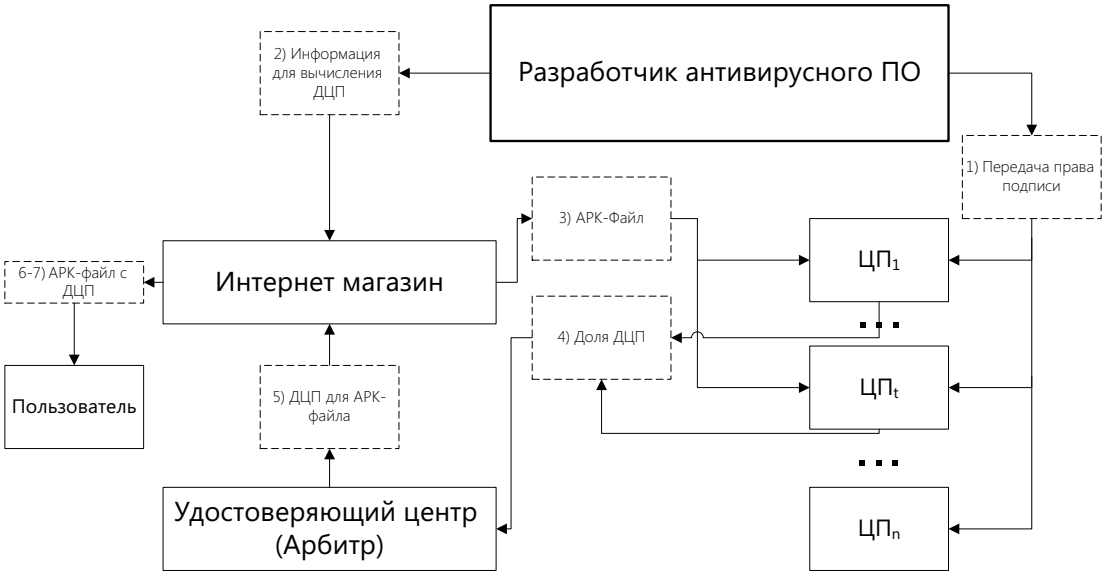

Рис. 1. Схема взаимодействия участников

(1,2 ГГц). В ходе тестирования, согласно данным приложения Android Assistant, использовалось только одно ядро многоядерных процессоров. Тестирование производилось на APK-файлах 5,3 и 76 Мбайт. В таблице для каждого из файлов указано время проверки 10000 ДЦП.

Процессор	**Файл 5,3 Мбайт**	**Файл 76 Мбайт**
Exynos 4412	97,4 с	1241,56 с
Exynos 4210	143,21 с	1785,56 с

ЛИТЕРАТУРА

1. *Толюпа Е. А.* Механизм антивирусной защиты на базе (n, t)-пороговой ДЦП с арбитром // МАИС. 2014 (в печати).
2. *Mambo M., Usuda K., and Okamoto E.* Proxy signatures for delegating signing operation // Proc. of 3rd ACM Conference on Computer and Communications Security (CCS'96). ACM Press, 1996. P. 48–57.

УДК 004.94

ДП-МОДЕЛЬ МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ С КОНТРОЛЕМ ЦЕЛОСТНОСТИ СУБД MySQL

Д. В. Чернов

Работа посвящена разработке механизмов мандатного контроля целостности в мандатной ДП-модели СУБД MySQL. Вводятся основные элементы модели (решётка уровней целостности сущностей, функции избирательности контроля целостности, уровней целостности сущностей и т. д.), с помощью которых обеспечивается мандатный контроль целостности; описываются некоторые правила преобразования состояний системы; определяются состояния системы, в которых не происходит нарушения целостности, и формулируются условия, которые необходимы, чтобы система оставалась в этих состояниях.

Ключевые слова: *управление доступом, мандатный контроль целостности, информационные потоки, формальные модели безопасности.*