EVALUATION OF STRESS CONCENTRATION IN THE CRANK ROD HEAD FORCED OF DIESEL

With increasing fatigue strength rod stock highly accelerated of diesel fatigue damage manifested at an earlier date determined by calculating the force. Fatigue fractures analysis showed that the nucleation of fatigue cracks observed within the transition at the edge portion in the region of the smallest cross section. This pattern of cracking indicates high level of operational voltage and the presence of a high concentration gradient.

Keywords: *margin of safety, fatigue fracture, cross-section, stress concentration, head of the piston rod.*

УДК 004.056.57

СПОСОБЫ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

М.В.Сухов[1], А.Ш. Бегалин[2],
кандидат технических наук, старший преподаватель,
Костанайский государственный педагогический институт[1],
магистр естественных наук, старший преподаватель,
Костанайский государственный университет имени А. Байтурсынова[2]

Положительные рецензии даны д.т.н. Боранбаевым С.Н. и к.т.н. Кудубаевой С.А.

Компьютерные вирусы, получившие широкое распространение в компьютерной технике, на сегодняшний день получили распространение и в мобильных устройствах, которыми мы пользуемся ежедневно, и уже не представляем, как без них можно обойтись. В статье рассмотрены основные разновидности мобильных вирусов и способов противодействия им.

Ключевые слова: *мобильные вирусы, вредоносные программы, антивирусная защита.*

Мобильные вирусы – это небольшие программы, предназначенные для вмешательства в работу мобильного телефона, смартфона, коммуникатора, планшета, которые записывают, повреждают или удаляют данные и распространяются на другие устройства через SMS и/или Интернет.

Впервые о мобильных вирусах заговорили ещё в 2000 году. Вирусами назвать их было тяжело, так как это был набор команд, исполняемый телефоном, который передавался через SMS. Такие

сообщения забивали соответствующие ячейки памяти и при удалении блокировали работу телефона. Наибольшее распространение получили команды для таких телефонов, как Siemens и Nokia.

Тенденция такова, что чем функциональнее телефон, тем большему количеству угроз он подвержен. Любые команды, функции и возможности, позволяющие создавать программы и приложения для мобильных телефонов, могут стать инструментом для создания вирусов. Наиболее перспективной платформой для написания вирусов является Java 2ME, так как подавляющее большинство современных телефонов поддерживает данную платформу.

Основной целью мобильных вирусов, как и в случае с компьютерными вирусами, является получение персональной информации, которую можно продать или использовать в личных нуждах. К такой информации могут относиться личные данные владельца телефона, данные самого устройства, личные сообщения, иногда номера кредитных карт [1].

Направления развития мобильных вирусов

Существует несколько различных схем и направлений развития вирусов, по которым действуют вирусописатели:

Кража персональной информации.

В данном случае вирусы собирают различные сведения, имеющиеся в телефоне, например, контакты владельца телефона, пароли от программ, параметры учетных записей, таких, как Google Play или AppStore. Вся информация, полученная вирусом, отправляется на сервер злоумышленников, где используется по их усмотрению. Один из самых серьезных вирусов такого плана – ***Android.Geinimi***. Попадая в систему, он определяет местоположение смартфона, загружает файлы из Интернета, считывает и записывает закладки браузера, получает доступ к контактам, совершает звонки, отправляет, читает и редактирует SMS-сообщения.

Отправка платных SMS-сообщений, звонки на «партнерский номер» без ведома владельца.

В данном случае за отправку сообщения или за звонок списывается серьезная сумма средств с лицевого счета владельца телефона. Разумеется, деньги попадают в руки злоумышленников. Из самых известных подобных угроз можно назвать ***Android.SMSSend***, а также давно известные ***RedBrowser*** и ***Webster*** для Java-платформы. Они маскируются под различные полезные программы, вызывая тем самым доверие у пользователя. Также существуют вирусы и для других платформ, например: Symbian OS, Windows Mobile и др.

Мошенничество посредством использованием систем интернет-банкинга.

В данном случае вирус открывает доступ к мобильному приложению для работы с банком или соответствующему веб-сайту, либо перехватывает SMS-сообщения, передаваемые пользователю от систем интернет-банкинга. Опасность данного типа может подстерегать владельцев мобильных телефонов, работающих на различных платформах. Известен

троян ***Trojan-Spy.SymbOS.Zbot.a***, работающий в совокупности с популярным вирусом ***Zbot*** для обычных ПК [2].

В июне 2004 года команда профессиональных вирусописателей 29A разработала первый в мире вирус для мобильных устройств – ***Caribe***. Это был червь для платформы Symbian, распространяющийся посредством Bluetooth. Никакого особого вреда, кроме как повышения расходования ресурсов аккумулятора, он не приносил, да и не должен был – команда 29A разработала этот вирус только для того, чтобы обратить внимание производителей ОС и антивирусного ПО на существенные бреши в системе безопасности Symbian. По поручению главы команды исходные коды Caribe были отправлены ведущим производителям антивирусов, однако вскоре в результате утечки они оказались и в открытом доступе. Это породило массовое распространение Caribe (или, по антивирусной классификации, вирус Cabir) и его клонов по смартфонам мира.

Немногим позже на чемпионате мира по лёгкой атлетике в Хельсинки произошла самая крупная локальная эпидемия мобильного вируса. На большом, переполненном людьми стадионе Cabir сумел распространиться почти моментально. Ситуацию смогли урегулировать специалисты финской антивирусной компании F-Secure: прямо на стадионе было организовано особое место, где сотрудники F-Secure удаляли Cabir из памяти смартфонов подходивших зрителей. Всего под воздействием Cabir и его модификаций оказалось более двадцати стран.

Эпидемия Cabir обратила внимание на проблему мобильной безопасности, однако, не пользователей, а вирусописателей. Через месяц после появления Cabir вышел вирус ***Duts*** – первый вирус для платформы Windows Mobile. Этот вирус имел способность заражать собой исполняемые файлы, однако перед заражением спрашивал разрешения у пользователя КПК или коммуникатора. Как мы видим, природа не обделила разработчиков Duts чувством юмора.

А вот следующий вирус для Windows Mobile – ***Brador*** – не был таким весёлым: это был первый в мире бэкдор для мобильной платформы. Brador ожидал подключения зараженного устройства к Сети, и как только оно было установлено, он отправлял IP-адрес устройства «хозяину» по e-mail и открывал для него особый порт. «Хозяин», подключившись через этот порт к инфицированному устройству, мог получить доступ к его файлам, самому отправлять ему те или иные файлы и выводить на его экран текстовые сообщения.

Впрочем, вирусы для Windows Mobile так и не получили особого распространения. Дело в том, что в то время доля Windows Mobile на рынке смартфонов и коммуникаторов не особо велика – тогда на этой ОС выпускались в основном КПК, которые находились подключенными к Сети крайне редко и мало. Так что пальму первенства в этой области держала платформа Symbian.

Очень долгое время пользователи не думали о защите своих мобильных устройств от вредоносного кода и наконец, пользователи

образумились. Они начали ставить антивирусные программы и файрволлы на свои смартфоны и коммуникаторы, они перестали загружать софт и игры из подозрительных источников, они начали ставить запреты на отправку SMS-сообщений Java-программами в настройках телефонов. Казалось, что компьютерные вирусы ушли навсегда... Однако на сцену вышла операционная система Android, и вирусописатели, «наложившись» на неё, породили такую эпидемию вирусов, которой мир ещё не видывал.

Система Android оказалась довольно уязвимой для вредоносных программ. В отличие от других Linux- и Unix-подобных систем, суперпользователь в «андроиде» не защищён паролем. Это, с одной стороны, облегчает жизнь пользователю (не надо вводить пароль при установке программ или выполнения иных важных действий), однако позволяет вирусам почти беспрепятственно получать доступ к важнейшим системным функциям. Суперпользователь в Unix и Linux – наиболее важный пользователь в системной иерархии, и именно от его имени совершаются все критические для системы действия. От имени суперпользователя можно даже перекомпилировать ядро. Таким образом, человек, не позаботившийся об установке антивируса на Android-устройство, по сути, «отдаёт» его злоумышленникам.

Есть и ещё одна причина, позволившая в таком масштабе распространиться вирусам на Android-приложения, которые поступают на проверку в Android Market, системный каталог приложений, не проходят премодерацию. Вследствие этого Android Market кишит низкокачественными поделками, «глючными» программами и «троянскими» приложениями. Поэтому необходимо всегда проявлять предельную осторожность, в том числе и при установке программ и игр из Android Market.

Число вредоносных программ, создающихся для Android, продолжает расти. По итогам января 2014 года количество уникальных экземпляров вредоносных программ для Android увеличилось на 34% по сравнению с декабрём 2013 года (в декабре 2012 года их насчитали 148 тысяч единиц). Коллекция вредоносных приложений для популярной мобильной ОС Android составляет более 10 миллионов экземпляров, сообщают специализированные издания. В 2012 году на самую популярную операционную систему в мире для смартфонов и планшетов пришлось 79% всех мобильных угроз. Еще 2011-м этот показатель составлял 66,7%, а в 2010-м – 11,25%.

Эксперты IDC считают, что засилье вредоносных программ на Android в ближайшем будущем будет только увеличиваться. По мнению F-Secure, меры безопасности, которые Google начала внедрять с версии 4.2 (Jelly Bean), могут помочь снизить эту цифру.

Самым распространенным видом угроз оказались трояны (66,1%) – программы, которые маскируются под «хорошие» приложения, но на самом деле воруют данные. Второе место заняли угрозы, навязывающие

платную подписку через SMS (11,2%). На третьем месте расположились вирусы-шпионы (7%) .

Защита от мобильных вирусов

Основное правило, которое поможет избежать попадания вирусов на мобильный телефон, гласит: «*Никогда не открывайте файлы, происхождение которых вам неизвестно, и которые, особенно, вызывают у вас подозрение*». Но, не смотря на это правило, порой даже самые осторожные люди попадаются на удочку хитрых и ловких разработчиков вирусов. Если в ваш мобильный телефон все же прокрался злостный вирус, вы можете попытаться избавиться от него следующим путем:

1. Выключите Bluetooth, GPS и Wi-Fi, закройте доступ для других пользователей. Если не помогает, извлеките SIM-карту чтобы избежать отсылки платных SMS с вашего номера.

2. Проверьте свою систему безопасности.

Попытайтесь отыскать в своих папках любой незнакомый для вас файл с подозрительным названием. Правда, это помогает не всегда, поскольку, например, вирус ***Commwarrior*** выбирает любое название для всех своих зараженных файлов. Однако, в большинстве случаев вирус все же можно вычислить по имени файла. В интернете можно также отыскать сайты, которые борются с распространением вирусов. Вы можете сделать заявку на одном из таких сайтов, и на ваш телефон пришлют полное описание вируса и способы борьбы с ним. Наиболее популярными считаются сайты – F-Secure, McAfee и Symantec.

3. Установите на мобильный телефон и регулярно обновляйте любой антивирусный программный продукт.

Многие компании разрабатывают программные средства защиты данных мобильных телефонов, некоторые из них можно бесплатно загрузить в интернете, другие можно только купить, также есть специальные программы, предназначенные только для мобильных операторов. Сразу после установления такие программы могут выявить и удалить вирус, и в дальнейшем защитить ваш телефон от проникновения некоторых видов вирусов. Компания Symbian специально разработала версию антивирусного программного продукта для защиты своей операционной системы, которая принимает только надежные файлы.

Помимо защиты от вредоносных приложений, мобильные антивирусы предлагают множество других полезных функций. К примеру, они могут удаленно заблокировать смартфон, если он был украден или потерян, или автоматически делать резервную копию контактов.

4. Избегайте установки приложений из сомнительных источников.

Во-первых, перед тем как скачать программу, всегда обращайте внимание на ее описание, рейтинг и отзывы других пользователей. Если она по каким-то причинам вызывает сомнения, то лучше от ее загрузки воздержаться и подыскать аналог. Строго не рекомендуется качать вручную APK-установщик из мест, которые не вызывают доверия.

Во-вторых, избегайте приложений малоизвестных создателей и с низкими оценками. В Google Play отличить подлинные программы от поддельных помогает отметка «лучший разработчик». Однако имейте в виду, что шанс нарваться на «троянца» есть и в «гугловском» маркете. К примеру, сейчас там размещен мошеннический «антивирус» Antivirus Free, который списывает со счета два доллара, отправляя платную SMS на короткий номер.

5. Не переходите по ссылкам от неизвестных отправителей.

Стоит всегда быть начеку и не нажимать на ссылки в письмах или SMS, которые пришли с незнакомых номеров. Даже если ссылку внезапно прислал знакомый контакт, лучше спросить о ней лично.

6. Защитите устройство паролем.

Задайте PIN-код. Кроме того, рекомендуется выполнить аппаратное шифрование всего содержимого смартфона. Это займет некоторое время, а также потребует ввода пароля каждый раз после перезагрузки, зато данные будут защищены. В настройках также желательно снять галку с пунктов «Показывать пароль», и «Неизвестные источники».

7. Не подключайтесь к подозрительным сетям W-Fi.

Некоторые хакеры намеренно разворачивают бесплатные точки доступа к Интернету и перехватывают трафик ничего не подозревающих пользователей. Чтобы не стать жертвой злоумышленников, избегайте общественных сетей, о которых вы не знаете. Кроме того, отключайте беспроводные модули Bluetooth, GPS и Wi-Fi, когда вы ими не пользуетесь.

И, конечно же, самое главное в защите мобильных устройств – это использование актуальных антивирусных программ.

ЛИТЕРАТУРА

1. Мобильная вирусология [Электронный ресурс] // Лаборатория Касперского. URL: http://www.securelist.com/ru/analysis/208050548/Mobilnaya_virusologiya_chast_3.

2. Антивирусное обеспечение: учеб. пособие / М.В. Сухов. – Костанай, 2013. – С.181.

3. Касперский К. Компьютерные вирусы изнутри и снаружи – Питер, 2006. –С. 526.

4. Касперский Е. «Компьютерное Zловредство». – Санкт-Петербург: Питер, 2007. - С.208:

ЗИЯН КЕЛТІРЕТІН БАҒДАРЛАМАЛАРДАН МОБИЛЬДЫҚ ҚҰРЫЛЫМДАРДЫҢ ҚОРҒАУЛАР ӘДІСТЕРІ

Компьютерлік техникада кең тараған компьютерлік вирустар, бүгінгі күні, біз күнделікті пайдаланып жүрген және онсыз қалай өмір сүретінімізді түсіне алмайтын ұялы құралдарда да тараған. Мақалада ұялы вирустардың негізгі түрлері мен оларға қарсы тұруды ңәдістері қарастырылған.

Түйін сөздер: *ұялы вирустар, зарарлы бағдарламалар, вирусқа қарсы қорғау*

WAYS TO PROTECT MOBILE DEVICES FROM MALWARE

The computer viruses which were widely adopted in the computer technics, for today were extended and in mobile devices which we use daily, and any more we do not represent, as without them it is possible to manage. In this publication the basic versions of mobile viruses and ways of counteraction are considered by it.

Keywords: *mobile viruses, malware, anti-virus protection*

УДК 681.142.2

OPTIMIZATION OF PRODUCTION PLANNING WITH LIMITED RESOURCES

А.А. Ташев[1], А.Н. Нургулжанова[2],
Doctor of technical sciences, professor[1],
Candidate of economical sciences, senior lecturer[2],
Kazakh academy of transport and communications by M.Tynyshpayev

Положительные рецензии даны д.т.н. Биттеевым Ш.Б.
и к.т.н. Кудубаевой С.А.

The problem of optimisation of planning of output which is reduced to a problem of linear programming is considered and solved by simplex method. The model for optimum planning of process production at the limited resources is offered.

Keywords: *optimum planning, output, model, the production, the limited resources.*

Let’s consider the production units, consisting of various production lines, where the output of each node can be used as input for other nodes.