НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н.Э. БАУМАНА
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408
электронный научно-технический журнал

Проблемы защиты мобильных персональных устройств от информационно-технического воздействия

 # 05, май 2012
DOI: 10.7463/0512.0404286

Захарчук И. И., Веселов Ю. Г., Еремеев М. А.

УДК 004.4

Россия, МГТУ им. Н.Э. Баумана
vesel_foto@mail.ru

Введение

В настоящее время технологическое развитие вносит новые коррективы в способы ведения вооруженного противоборства. Реализация сетецентрического подхода к организации управления ведением военных действий предусматривает беспрецедентную вертикальную и горизонтальную информационную интеграцию ключевых элементов вооруженных сил с использованием современных технологий сбора, обработки, хранения и передачи информации [1]. Построение такой глобальной автоматизированной системы в рамках всех вооруженных сил ставит целый ряд проблем связанных с интеграцией большого числа узкоспецифических систем, обслуживающих различные виды и роды войск. При этом к каждому элементу системы предъявляются дополнительные требования, обусловленные общими тактико-техническими характеристиками системы, прежде всего в области защиты обрабатываемой информации.

Рассматривая элементы сетецентрической системы можно выделить класс портативных индивидуальных устройств, которые будут непосредственно использоваться военнослужащими на поле боя - мобильные персональные устройства (МПУ). Отличительными предъявляемыми к ним требованиями являются легкость использования, компактность и портативность [1, 2]. В целом, класс таких устройств весьма обширен. В него включаются смартфоны, планшеты, карманные персональные компьютеры, навигаторы и прочие портативные и

миниатюрные вычислительные устройства. При этом тенденция увеличения объема циркулирующего информационного потока, применение современных средств связи (аудио и видео), средств криптозащиты и контроля функционирования ставит серьезную преграду для разработчиков МПУ с точки зрения обеспечения производительности. Использование портативных источников питания дополнительно накладывает ограничения, не позволяя решить проблему обеспечения производительности МПУ простым наращиванием вычислительных мощностей. Наиболее перспективным направлением представляется поиск новых методов и алгоритмов обработки информации в МПУ.

Развитие современных средств информационной борьбы предъявляет особые требования к организации вычислительного процесса в МПУ с точки зрения обеспечения информационной безопасности, учитывая, что МПУ является частью автоматизированной системы военного назначения (АС ВН). Рассматривая МПУ с этой позиции, следует отметить ряд присущих им особенностей, а именно:

1. Большой объем и разнородность обрабатываемой конфиденциальной информации.
2. Подключение к различным каналам связи, в том числе к общественным (недоверенным).
3. Наличие в МПУ дополнительного оборудования такого как камера, GPS/ГЛОНАСС, микрофон и других.

Суммируя, отметим, что МПУ отличаются повышенными требованиями к обеспечению безопасности при ограниченных возможностях её обеспечения. Наличие этого критического противоречия толкает разработчиков мобильных устройств искать новые подходы к обеспечению безопасности.

Целью статьи является обзор существующих видов информационного воздействия на МПУ, а также механизмов их защиты. В статье были впервые рассмотрены механизмы защиты неспециализированных «гражданских» МПУ с позиции их дальнейшей интеграции в единую информационную среду в рамках сетецентрического подхода построения перспективных АС ВН.

Виды воздействий на МПУ

Все существующие методы защиты МПУ можно разделить на два класса - защита канала связи МПУ, что косвенно относится к защите самого МПУ, и, собственно, защита самого МПУ как аппаратно-программного комплекса обработки информации [3]. С точки зрения обеспечения информационной безопасности как обеспечения составляющих её целостности, конфиденциальности и доступности информации, защиту МПУ можно рассматривать по этим соответствующим трем направлениям (см. рисунок).

Рисунок - Виды воздействий на мобильный сегмент

Анализ современных методов защиты МПУ

В настоящее время производители МПУ прилагают усилия для комплексной защиты производимых устройств, причем как в совершенствовании аппаратной части, так и, в большей степени, программной. При этом большая часть мер защиты обеспечивает сразу несколько направлений, взаимно дополняя друг друга на разных уровнях и повышая общую защищенность системы. Говоря о мерах защиты, следует отметить, что архитектура современных операционных систем для МПУ изначально разрабатывалась со встроенными в нее механизмами

обеспечения безопасности. Однако непрерывное развитие современных средств информационного воздействия постепенно снижают эффективность защиты, заставляя разрабатывать все более совершенные защитные механизмы. Наиболее значимыми из них являются:

- технологии изолирования («sandboxing»),
- шифрования памяти МПУ,
- технология рандомизации адресного пространства (ASLR).

Технология изолирования заключается в использовании запускаемыми программами ресурсов операционной системы через «прослойку» специальной системы управления доступом («песочница», «sandbox»). Для выполняемой программы система управления доступом создает ограничения по использованию ресурсов операционной системы исходя из понятий «типичного» и «нетипичного» поведения конкретной исполняемой программы [4]. Например, при нормальной работе графическому редактору не требуется доступ к Интернету или к хранилищу учетных записей пользователей и паролей к ним. Таким образом, исходя из реальных «типичных» потребностей программы, система управления доступом разрешает использование только необходимых ресурсов.

Такой подход позволяет в случае взлома исполняемой программы или наличия в ней недекларируемых возможностей не допустить компрометации всей системы и всех её ресурсов [4-6]. В идеале, сам разработчик ПО должен позаботиться об ограничении допустимых действий своей программы. Однако, если такие ограничения отсутствуют, «песочница» нивелирует просчеты или умышленные закладки разработчика программного обеспечения, а также найденные впоследствии в нём уязвимости. Данный подход в настоящее время реализован в таких программных продуктах как Google Chrome, Microsoft Office 2010, Adobe Reader X и многих других [5]. Все современные операционные системы МПУ, такие как Android, iOS, Windows Phone 7 разработаны с внедренными в них подобными системами управления доступом.

Использование криптографических средств защиты позволяет обеспечить конфиденциальность информации как при попытке удаленного считывания информации с помощью внедренных в ОС МПУ специальных программных средств, так и при попытке локального считывания информации из внутренней памяти устройства.

В силу того, что шифрование всей памяти МПУ при современных нормах от нескольких до десятков гигабайт требует значительных ресурсов, в миниатюрных устройствах применяют аппаратные модули шифрования.

Например, в смартфоне IPhone 3GS, работающего под управлением ОС iOS 3, с помощью «прозрачного» для операционной системы шифрования всей внутренней памяти устройства обеспечивалась возможность быстрого безвозвратного стирания информации в случае, например, кражи смартфона [7]. По специальной команде извне смартфон стирает уникальные для каждого экземпляра устройства ключи шифрования, лишая смысл считывание зашифрованной памяти. В качестве алгоритма шифрования применяются, как правило, разновидности алгоритма AES - главным образом, из-за отработанной технологии реализации этого алгоритма в криптосопроцессорах, что позволяет многократно увеличить скорость шифрования/дешифрования.

Начиная с мобильной ОС iOS 4 применяется более мощная система криптозащиты. iOS 4 получила специальную систему хранения паролей (keybag) - каждый файл файловой системы шифруется индивидуальным ключем. Таким образом, при вскрытии ключа шифрования какого-либо отдельного файла компрометации всей информации не происходит. Сами ключи хранятся в keybag зашифрованные мастер-ключем, который в свою очередь генерируется на основе уникального идентификатора устройства и пароля, установленного пользователем. Привязка к уникальному идентификатору МПУ делает возможной генерацию мастер-ключа лишь на самом МПУ, и таким образом попытки подобрать мастер-ключ перебором, распараллеливая процесс между несколькими устройствами для достижения приемлемого времени нахождения ключа , становятся невозможными.

Технология защиты ASLR (Address space layout randomization) заключается в размещении частей программы случайным образом в адресном пространстве вычислительного устройства. Такими частями являются образ самого исполняемого файла, подгружаемые библиотеки, «куча» (heap) и стека. Технология ASLR значительно усложняет успешную эксплуатацию нескольких типов уязвимостей [8]. Например, даже если при помощи переполнения буфера или другим методом

атакующий получит возможность передать управление по произвольному адресу, ему нужно будет угадать, где же именно расположен стек или куча или другие места в памяти в которые он может поместить шелл-код. Важно отметить, что ASLR подразумевает под собой лишь общую идею, технологический подход к защите системы. Реализация технологии ASLR на различных операционных системах может сильно отличаться как по сложности и влиянию на производительность системы, так и по степени защиты от атак. Здесь под степенью защиты понимают вероятность угадывания атакующим расположения сегментов взламываемой программы.

При попытках применения ASLR в мобильных устройствах, как, впрочем, и при попытках применения других технологий, заимствованных из мира настольных компьютеров, перед разработчиками возникают проблемы сохранения приемлемого уровня быстродействия мобильных устройств. Рассматривая операционную систему Android, можно отметить, что в ней для решения проблемы быстродействия приложений был введен запускаемый при загрузке мобильного устройства процесс «zygote», который содержит в себе экземпляры общесистемных библиотек, окружений и виртуальной машины Dalvik. При запуске приложения, система делает копию уже загруженных в память проинициализированных ресурсов, таким образом заметно выигрывая в скорости запуска. Отсюда вытекает, что для всех установленных на мобильном устройстве приложений параметры расположения системных ресурсов будут одними и теми же. Впрочем, как утверждают разработчики Android 4, реализация ASLR в этой мобильной ОС была предназначена для усложнения потенциальных сетевых атак на устройство. Однако, несмотря на все вышеизложенные недостатки, ASLR остаётся достаточно эффективной технологией информационной защиты.

Помимо приведенных выше, существует еще ряд приемов, повышающих общую защищенность МПУ. К ним можно отнести подписывание устанавливаемых приложений и обновлений операционной системы электронной цифровой подписью (ЭЦП) в целях идентификации источника ПО и проверки целостности программного кода. В дальнейшем, исходя из результатов проверки ЭЦП и политики безопасности, устанавливаемой разработчиком ОС, применяется решение о допустимости или недопустимости установки ПО. Например

iPhone под управлением ОС iOS позволяет устанавливать только ПО, подписанное разработчиком - компанией Apple. ОС Android позволяет пользователю самому решать, устанавливать неподписанные пользовательские приложения или нет, при этом исключительное право на установку системного ПО остается за производителем МПУ.

Заключение

Оценивая существующие методы защиты МПУ от информационно-технических воздействий, можно прийти к выводу, что при всем многообразии применяемых методов и средств, по настоящему универсального метода защиты МПУ, способного обеспечивать необходимый уровень комплексной защищенности при сохранении с другой стороны требуемого уровня производительности и удобства пользования устройством, пока не существует [9]. Использование взаимоинтегрированных социальных, платежных и других сетевых сервисов, средств синхронизации данных между устройствами, сетевых ГИС и интегрированных с ними автоматизированных систем управления поднимает проблему учета и разграничения доступа к данным различной степени важности и конфиденциальности. В дальнейшем, при наличии большого числа устройств, в том числе мобильных, а также при большом числе уровней разграничения доступа к данным и разнородности самих данных, недоверие к надежности и защищенности МПУ и общая сложность системы создают перед разработчиками информационных систем иллюзию невозможности сохранения всех функций коммуникации и взаимодействия с внешним миром, заложенных разработчиком устройства. Вот почему крайне актуальной является задача разработки новых эффективных методов комплексной защиты информационных систем, которые будут максимально «прозрачны» для ПО и конечных пользователей.

Литература

1. David A. Fritz, Bharat T. Doshi, Andrew C. Oak, Harry L. Miller, John D. Oetting, Ryan M. Collins and others. Military Satellite Communications: Space-Based Communications for the Global Information Grid // Johns Hopkins APL Technical Digest. 2006. vol. 27.

№. 1. pp. 32-40.
2. The Global Information Grid and Challenges Facing Its Implementation. URL: http://www.gao.gov/products/GAO-04-858 (дата обращения: 22.02.2012).
3. Б. Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Питер, Спб, 2003. 368 с.
4. Dionysus Blazakis. The Apple Sandbox, 2011. URL: http://dl.packetstormsecurity.net/papers/general/apple-sandbox.pdf (дата обращения: 22.02.2012).
5. Tom Keetch. Practical Sandboxing on the Windows Platform, A technical white paper for the Black Hat Briefings, Europe 2011. URL: https://media.blackhat.com/bh-eu-11/Tom_Keetch/ /BlackHat_EU_2011_Keetch_Sandboxes-Slides.pdf (дата обращения: 05.03.2012).
6. Security Engineering Research Group. Analysis of Dalvik Virtual Machine and Class Path Library, 2009. URL: http://serg.imsciences.edu.pk (дата обращения: 5.03.2012).
7. Andrey Belenko, Dmitry Sklyarov. Evolution of iOS Data Protection and iPhone Forensics: from iPhone OS to iOS 5, Blackhat Abu Dhabi Conference, 2011. URL: https://media.blackhat.com/bh-ad-11/Belenko/bh-ad-11-Belenko-iOS_Data_Protection.pdf (дата обращения: 5.02.2012).
8. Hristo Bojinov, Dan Boneh, Rich Cannings, Iliyan Malchev. Address Space Randomization for Mobile Devices. URL: http://research.google.com/pubs/archive/37656.pdf (дата обращения: 12.02.2012).
9. Alessandro Distefano, Gianluigi Me, Francesco Pace. Android anti-forensics through a local paradigm. URL: http://www.dfrws.org/2010/proceedings/2010-310.pdf (дата обращения 3.02.2012).

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU
SCIENCE and EDUCATION
EL № FS 77 - 48211. №0421200025. ISSN 1994-0408
electronic scientific and technical journal

Mobile personal device information security problems

 # 05, May 2012
DOI: 10.7463/0512.0404286

Zaharchuk I.I., Veselov Yu., G., Eremeev M.A.

Russia, Bauman Moscow State Technical University
vesel_foto@mail.ru

The paper describes the main types of threats to the mobile segment of the perspective military information infrastructure. The main principal approaches and technologies of mobile device security were analyzed.

Publications with keywords: mobile devices, network-centric warfare (NCW), mobile device security, information technology security
Publications with words: mobile devices, network-centric warfare (NCW), mobile device security, information technology security

References

1. David A. Fritz, Bharat T. Doshi, Andrew C. Oak, Harry L. Miller, John D. Oetting, Ryan M. Collins, et al. Military Satellite Communications: Space-Based Communications for the Global Information Grid. *Johns Hopkins APL Technical Digest*, 2006, vol. 27, no. 1, pp. 32-40.

2. *The Global Information Grid and Challenges Facing Its Implementation*. Available at: http://www.gao.gov/products/GAO-04-858 , accessed 22.02.2012.

3. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000, 432 p. (Russ. ed.: Shnaier B. *Sekrety i lozh'. Bezopasnost' dannykh v tsifrovom mire*. St. Petersburg, Piter, 2003. 368 c.).

4. Blazakis D.. *The Apple Sandbox*. Available at: http://dl.packetstormsecurity.net/papers/general/apple-sandbox.pdf , accessed 22.02.2012.

5. Keetch T. *Practical Sandboxing on the Windows Platform, A technical white paper for the Black Hat Briefings, Europe 2011*. Available at: https://media.blackhat.com/bh-eu-11/Tom_Keetch/ /BlackHat_EU_2011_Keetch_Sandboxes-Slides.pdf , accessed 05.03.2012.

6. *Security Engineering Research Group. Analysis of Dalvik Virtual Machine and Class Path Library*. Available at: http://serg.imsciences.edu.pk , accessed 5.03.2012.

7. Belenko A., Sklyarov D. Evolution of iOS Data Protection and iPhone Forensics: from iPhone OS to iOS 5. *Blackhat Abu Dhabi Conference*, 2011. Available at: https://media.blackhat.com/bh-ad-11/Belenko/bh-ad-11-Belenko-iOS_Data_Protection.pdf , accessed 5.02.2012.

8. Bojinov H., Boneh D., Cannings R., Malchev I. *Address Space Randomization for Mobile Devices*. Available at: http://research.google.com/pubs/archive/37656.pdf , accessed 12.02.2012.

9. Distefano A., Me G., Pace F. *Android anti-forensics through a local paradigm*. Available at: http://www.dfrws.org/2010/proceedings/2010-310.pdf , accessed 3.02.2012.