Моделирование и анализ компонентов удаленной аттестации Android-приложений для систем Интернета вещей

В. А. Десницкий[1], И. В. Котенко[2]
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)
[1]desnitsky@comsec.spb.ru, [2]ivkote@comsec.spb.ru

***Аннотация*. В работе моделируются механизмы защиты Android-приложений систем Интернета вещей от угроз нарушения целостности программного кода и критически важных данных на основе принципов удаленной аттестации. Аттестация базируется на контроле потока управления и проверке контрольных сумм заданных структур данных. В частности, на уровне исходного кода конкретного приложения расставляются программные маркеры. После этого формируется регулярное выражение, определяющее корректные потоки управления защищаемой программы, на основе чего на аттестующей стороне формируется граф для проверки аттестующих данных. Проводятся аналитическая и экспериментальная оценки реализованных компонентов защиты и протокола их взаимодействия с учетом ограничений на вычислительные и коммуникационные ресурсы целевого устройства.**

Ключевые слова: удаленная аттестация; целостность; мобильное приложение; Интернет вещей

I. Введение

Проблема защиты программного обеспечения систем Интернета вещей от угроз несанкционированной модификации приобретает все более важный характер и обуславливается подверженностью программного обеспечения платформ мобильных и встроенных устройств, таких как Android, Raspberry Pi и др. угрозам нарушения целостности и аутентичности программного кода и используемых данных.

В общем случае применение алгоритмов контроля неизменности программного обеспечения, встраиваемых непосредственно в защищаемую ими программу, позволяет повысить уровень ее защищенности. Однако локальный характер действия защиты и ограничения ее стойкости, а также нахождение программы в не доверенном и неконтролируемом со стороны разработчика ПО или владельца прав на него окружении приводит к тому, что такие механизмы защиты могут быть нейтрализованы нарушителем при наличии достаточных для этого средств и ресурсов. Исследуемый в работе механизм удаленной аттестации базируется на использовании клиент-серверного подхода к защите и позволяют повысить защищенность программного обеспечения в условиях ресурсных ограничений устройств мобильных платформ, а также ограничений пропускной способности имеющихся коммуникационных каналов.

В работе проведены моделирование и анализ частных алгоритмов защиты в рамках комплексного подхода к реализации компонентов защиты программного обеспечения, реализующих принципы удаленной аттестации на примере устройств платформы Android. К отличительным особенностям результатов работы относятся, в частности, экспериментальные оценки, полученные в процессе моделирования компонентов защиты в условиях ограничений мобильных операционных систем.

Статья включает следующие основные разделы. В разделе 2 приведен обзор существующих работ в предметной области. В разделе 3 раскрываются особенности исследуемого подхода к удаленной аттестации мобильных приложений. В разделе 4 описаны результаты моделирования конкретных алгоритмов, реализующих принципы удаленной аттестации. В разделе 5 представлены результаты экспериментальных исследований и выводы. Раздел 6 служит заключением статьи.

II. Релевантные работы

В [1–2] удаленная аттестация рассматривается как средства защиты против атак внедрения вредоносных программ на встроенные устройства [3]. Показаны особенности и методы, позволяющие реализовать аттестацию с минимальными дополнительными затратами. При этом Preschern и др. в [2] предлагают адаптацию программных методов удаленной аттестации для решения задач защиты критически важных систем с минимальным вынужденным пересмотром установленных процедур сертификации свойств надежности.

В [4] удаленная аттестация используется для выявления само распространяющихся сетевых червей в сенсорных сетях путем последовательного инфицирования узлов с применением методов детектирования трафика.

Работа выполнена при частичной финансовой поддержке проектов РФФИ (№ 16-29-09482 и 18-07-01488), гранта Президента Российской Федерации № МК-5848.2018.9 и бюджетной темы №. АААА-А16-116033110102-5.

Srinivasan и др. исследуют основанную на программных методиках удаленную аттестацию для обеспечения целостности ядра операционной системы и пользовательских приложений. В частности, предложена методика, позволяющая установить, было ли уже аттестованное приложение подменено нарушителем или нет [5].

В [6] предлагаются использование удаленной аттестации и построенной на ее основе трех фазный протокол с использованием модуля SELinux для обеспечения защищенного взаимодействия в распределенных информационных системах. В работе также обосновывается эффективность предложенного подхода с использованием методов формального анализа и верификатора ProVerif.

В [7] предлагаются программные методики удаленной аттестации беспроводных сенсорных сетей от атак вмешательства в их работу. Данные методики не базируются на использовании фактора точности измеряемого времени выполнения, в результате чего позволяют улучшить предложенные ранее способы контроля целостности в беспроводных сенсорных сетях [8]. В [9] проводится анализ защищенности механизмов одно- и много-хоповой аттестации в беспроводных сенсорных сетях.

В [10] предложен многоуровневый протокол удаленной аттестации для контроля целостности IoT-систем с учетом присущих им вычислительных ограничений и ограничений мощности устройств.

В [11], [12] предлагается общая архитектура и частные модели для механизмов удаленной аттестации IoT-систем с использованием облачных решений для улучшения целевых показателей процесса удаленной аттестации. В [13] обосновывается важность удаленной аттестации с использованием облачных вычислений и процедур проверки ее корректности при выполнении обновлений ПО [14].

В [15] Zhang и др. расширяют действенность удаленной аттестации в целях обеспечения конфиденциальности при помощи модифицированного алгоритма EHA [16] с достижением повышенного уровня конфиденциальности при сравнимых характеристиках производительности в процессе выполнения.

В [17] предлагаются эффективные решения для повышения масштабируемости механизмов удаленной аттестации множеств устройств с использованием технологии Больших Данных, в том числе с использованием многопроцессорных систем [18], механизмов аутентификации на основе свойств [19] и характеристик этих свойств [20]. Повышение эффективности серверной части механизма аутентификации при большом числе экземпляров аттестуемых программ достигается также за счет реорганизации и уменьшения цепочки доверия, используемой в процессе аттестации [21].

В [22] предлагаются модели удаленной аттестации на основе парадигме программных графов атак в контексте направления задач мониторинга и аттестации программных компонентов [23].

III. Подход к удаленной аттестации мобильных приложений

Удаленная аттестация мобильного приложения включает программные локальный и удаленный компоненты, располагающиеся в рамках не доверенного и доверенного окружения, соответственно, а также защищенный протокол их сетевого взаимодействия. Взаимодействие между компонентами осуществляется на основе ролей клиента – аттестуемой сущности и сервера – аттестующей с реализацией функций защиты самого протокола от возможного перехвата и модификации пакетов на транспортном уровне. Полезная нагрузка протокола включает программные идентификаторы и числовые значения, характеризующие текущее состояние элементов программного кода и критически важных данных защищаемого приложения.

Конкретные алгоритмы, используемые в рамках механизма защиты на основе принципов удаленной аттестации, предполагают внедрение специфичных конструкций, внедряемых в объектный код на этапе формирования синтаксического дерева приложения и выделение в коде базовых блоков и отдельных инструкций.

Защитные конструкции непосредственно не осуществляют какую-либо проверку целостности кода и данных локально, а отправляют их слепки на сторону доверенного сервера, что значительно затрудняет возможность нарушителя модифицировать приложение без его последующего выявления на серверной стороне.

Типовой сценарий применения удаленной аттестации для защиты мобильных устройств подразумевает удаленный контроль со стороны магазина мобильных приложений или контент-провайдера над множеством экземпляров клиентских приложений с возможностью сигнализации о выявленных нарушениях на конкретных устройствах и прекращении их дальнейшего сопровождения до момента устранения выявленного нарушения.

IV. Алгоритмы защиты

Алгоритм контроля потока управления базируется на графе потока управления защищаемой программы, построенном статически, который используется в динамике для удаленного контроля корректности процесса ее выполнения. Данный алгоритм позволяет гарантировать правильность выполнения последовательности команд, в том числе конструкций ветвления, циклов, обработки исключительных ситуаций и др.

Алгоритм контроля потока управления включает две стадии – статическую и динамическую. Статически производится подготовка и встраивание в программный код конструкций аттестующего модуля. Инициирующая конструкция осуществляет установление соединения с удаленным контролирующим модулем посредством HTTP-

сокетов. Программные маркеры, представляющие собой операции отправки *send(A)* специфического идентификатора *A* на серверную сторону расставляются в программном коде на границе базовых блоков. В функцию аттестующего модуля на клиентской стороне входит отправка последовательности идентификаторов программных маркеров при их прохождении в процессе выполнения (динамически).

На серверной стороне соединения в рамках статической стадии производится построение регулярного выражения, определяющего корректные цепочки срабатывания программных маркеров. На основе регулярного выражения строится граф переходов, узлами которого служат программные маркеры, а дугами – допустимыми переходы между ними. На динамической стадии осуществляется процесс обхода графа при получении с клиентской стороны идентификаторов программных маркеров и проверка их корректности в соответствии со структурой графа. В качестве примера на рис. 1 схематично показан фрагмент программного кода защищаемой программы со встроенными функциями отправки программных маркеров.

```
send("A");
while(t<=250){
    send("B");
    if(checkLicenseCode()){
        setDependMode();
        send("C");
    } else {
        // business code
        send("D");
    }
    runEmerging();
    t++;
    send("E");
}
send("F");
```

Рис. 1. Фрагмент программного кода защищаемой программы

Регулярное выражение в инфиксной записи, построенное для данного фрагмента на серверной стороне, имеет вид *A(B(C|D)E)*F*. Соответствующий данному регулярному выражению граф переходов с финальной вершиной *F* показан на рис. 2.

Алгоритм проверки контрольных сумм предполагает наличие инвариантных структур данных, имеющих критически важный характер по отношению к задаче обеспечения целостности защищаемого программного кода и данных. В качестве основы используется криптографический алгоритм MD5. Отправка на серверную сторону соединения и проверка полученного токена осуществляется при помощи функций *send(md5(criticulStructure))* и *verify(getNextToken())*, соответственно.

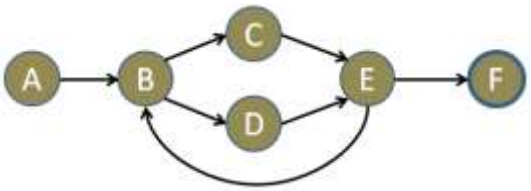

Рис. 2. Граф переходов для работы алгоритма удаленной аттестации

V. Эксперименты и дискуссия

Оценка построенных в работе решений производится путем определения и анализа значений ряда показателей, а именно показателей оперативности, достоверности и ресурсопотребления [24].

Показатель оперативности обуславливается наличием аппаратных ограничений платформы Android и ограничением пропускной способности коммуникационного канала, которые влияют на стабильность и бесперебойность работы приложения, а также на удобство использования (usability) со стороны конечного пользователя. Показатель оперативности вычисляется на тестовом сценарии с использованием системной функции *System.currentTimeMillis*, как усредненное значение временных задержек, возникающих в результате выполнения команд отправки программных маркеров и контрольных сумм.

Результаты проведенных экспериментов показали, что при соотношении числа встраиваемых инструкций аттестующего модуля к числу инструкций целевой программы не превышающем 20% усредненное значение задержек не превысило установленный допустимый предел в 200 мс.

Вычисление показателей ресурсопотребления производится с использованием утилит jmap и jstat, позволяющих оценить увеличение расхода ресурса потребляемой оперативной памяти на клиентской стороне при добавлении функций аттестации в программный код. На основе серии измерений, произведенных на тестовом приложении, определено, что увеличение расхода оперативной памяти не превысило 21% по сравнению с незащищенным вариантом программного приложения.

Для оценки показателя достоверности предложенного защитного решения проводилось fuzzy-тестирование защищенного приложения на заранее сформированных тестовых, в том числе случайных и граничных значениях входных данных. Тестирование на серии 250 образцах входных данных выявило отсутствие ошибок первого и второго рода, что подтверждает корректность предложенного подхода к удаленной аттестации и работоспособность ее программной реализации.

Применимость предлагаемого подхода к защите целостности Android-приложений обуславливается также достижимым уровнем автоматизации разворачивания предлагаемых защитных решений, в том числе выбором местоположения и расстановкой аттестующих команд в рамках защищаемого программного кода. Это обуславливает решение вопросов эффективного подбора и

адаптации существующих программных инструментов обработки Java-кода, как на уровне исходных текстов, так и непосредственно с использованием средств анализа байт-кода.

VI. Заключение

Проведено исследование подхода к удаленной аттестации мобильных приложений с использованием алгоритмов контроля потока управления и проверки контрольных сумм. Проведена программная реализация алгоритмов на примере платформы Android, которая использовалась в качестве основы для получения экспериментальных оценок данных алгоритмов. В качестве направления будущих исследований планируются развитие путей анализа защищенности мобильных приложений и повышение их защищенности, в том числе на уровнях исходного и объектного кода приложений.

Список литературы

[1] Brasser F., Rasmussen K.B., Sadeghi A.R., Tsudik G. Remote attestation for low-end embedded devices: The prover's perspective // 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC). Austin, TX. 2016. P. 1-6.

[2] Preschern C., Hormer A.J., Kajtazovic N., Kreiner C. Software-Based Remote Attestation for Safety-Critical Systems // 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation. Workshops, Luxembourg. 2013. P. 8-12. DOI: 10.1109/ICSTW.2013.7.

[3] Desnitsky V., Chechulin A., Kotenko I., Levshun D., Kolomeec M. Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System // 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2016). Heraklion. Crete. Greece. IEEE Computer Society. 2016. P.609-616. DOI: 10.1109/PDP.2016.99.

[4] Ho J.W., Wright M. Distributed Detection of Sensor Worms Using Sequential Analysis and Remote Software Attestations // IEEE Access. Vol. 5. 2017. P. 680-695.

[5] Srinivasan R., Dasgupta P., Gohad T. Software Based Remote Attestation for OS Kernel and User Applications // 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust. 2011 IEEE Third International Conference on Social Computing. Boston, MA. 2011. P. 1048-1055.

[6] Santra M., Peddoju S.K., Bhattacharjee A.K., Khan A. Design and Analysis of a Modified Remote Attestation Protocol // 2017 IEEE Trustcom/BigDataSE/ICESS. Sydney, NSW. 2017. P. 578-585. DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.287.

[7] AbuHmed T., Nyamaa N., Nyang D. Software-Based Remote Code Attestation in Wireless Sensor Network // 2009 IEEE Global Telecommunications Conference (GLOBECOM 2009). Honolulu. HI. 2009. P. 1-8.

[8] Xiangying K., Yanhui C. Dynamic Remote Attestation Based on Concerns // 2015 8th International Symposium on Computational Intelligence and Design (ISCID). Hangzhou. 2015. P. 76-80. DOI: 10.1109/ISCID.2015.120.

[9] Fu D., Peng X. TPM-based remote attestation for Wireless Sensor Networks // Tsinghua Science and Technology. Vol. 21. No. 3. 2016. P. 312-321.

[10] Tan H., Tsudik G., Jha S. MTRA: Multiple-tier remote attestation in IoT networks // 2017 IEEE Conference on Communications and Network Security (CNS). Las Vegas, NV. 2017. P 1-9.

[11] Song H., Fink G.A., Jeschke S. Secure Registration and Remote Attestation of IoT Devices Joining the Cloud: The Stack4Things Case of Study // Security and Privacy in Cyber-Physical Systems:Foundations, Principles, and Applications. Wiley-IEEE Press. 2017. P. 472. DOI: 10.1002/9781119226079.ch7.

[12] Azadiabad S., Pedram H., Abbasy M.R. Scalable protocol for remote integrity attestation of cloud based distributed services // 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT). Astana. 2014. P. 1-5. DOI: 10.1109/ICAICT.2014.7035912.

[13] Ramachandran K., Lutfiyya H. A remote attestation infrastructure for verifying the application of software updates // 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Lisbon. 2017. P. 317-325.

[14] Desnitsky V., Kotenko I. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // 4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). Fribourg. Switzerland. Lecture Notes in Computer Science (LNCS). Vol. 8708. Springer-Verlag. 2014. P.194-210.

[15] Zhang Y., Wang L., You Y., Yi L. A Remote-Attestation-Based Extended Hash Algorithm for Privacy Protection // 2017 International Conference on Computer Network, Electronic and Automation (ICCNEA). Xi'an. 2017. P. 254-257.

[16] Xiangying K., Yanhui C. Left full binary hash tree for remote attestation // 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP). Singapore. 2017. P. 385-390.

[17] Syed T. A., Jan S., Musa S., Ali J. Providing efficient, scalable and privacy preserved verification mechanism in remote attestation // 2016 International Conference on Information and Communication Technology (ICICTM). Kuala Lumpur. 2016. P. 236-245. DOI: 10.1109/ICICTM.2016.7890807.

[18] Kiperberg M., Resh A., Zaidenberg N.J. Remote Attestation of Software and Execution-Environment in Modern Machines // 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing. New York, NY. 2015. P. 335-341.

[19] Liang Y., Guo K.E., Li J. The remote attestation design based on the identity and attribute certificates // 2014 11th International Computer Conference on Wavelet Actiev Media Technology and Information Processing (ICCWAMTIP). Chengdu. 2014. P. 325-330. DOI: 10.1109/ICCWAMTIP.2014.7073419.

[20] Francillon A., Nguyen Q., Rasmussen K.B., Tsudik G. A minimalist approach to Remote Attestation // 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden. 2014. P. 1-6. DOI: 10.7873/DATE.2014.257.

[21] Luo W., Liu W., Luo Y., Ruan A., Shen Q., Wu Z. Partial Attestation: Towards Cost-Effective and Privacy-Preserving Remote Attestations // 2016 IEEE Trustcom/BigDataSE/ISPA. Tianjin. 2016. P. 152-159. DOI: 10.1109/TrustCom.2016.0058.

[22] Li H., Wang S. An Efficient and Flexible Dynamic Remote Attestation Method // 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications. Guangdong. 2014. P. 239-246.

[23] Meng C., He Y., Zhang Q. Remote Attestation for Custom-built Software // 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing. Wuhan. Hubei. 2009. P. 374-377.

[24] Desnitsky V., Kotenko I. Modeling and Analysis of IoT Energy Resource Exhaustion Attacks // Intelligent Distributed Computing XI. Studies in Computational Intelligence. Springer-Verlag. Vol.737. Proceedings of 11th International Symposium on Intelligent Distributed Computing (IDC'2017). Belgrade. Serbia. 2017. Springer-Verlag. 2017. P. 263-270.